NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

IT-21 COMPLIANT CONTROLLED ACCESS TO INTERNET WEB PAGES

by

Marcia S. Sonon

September 1998

Thesis Advisor: Gus K. Lott
Second Reader: Daniel F. Warren

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 1998	Master's Thesis

4. TITLE AND SUBTITLE
IT-21 COMPLIANT CONTROLLED ACCESS TO INTERNET WEB PAGES

5. FUNDING NUMBERS

6. AUTHOR(S)
Sonon, Marcia S.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

Although numerous resources are available to achieve Internet presence by creating and publishing a web site, security and access control within the site are very limited. The Navy's support of the IT-21 initiative embracing the Microsoft® Windows NT® operating system (OS) provides solutions to not only restrict entry to the site, but also to control access to content on the web page.

Work detailed in this thesis addresses the issue of security by exploring the Windows NT OS and activating its inherent security features to protect the overall system from intrusion and attacks from the internet. The web pages are published using Microsoft® Internet Information Server 4.0 (IIS) and FrontPage™ 98. Access is controlled by issuing certificates from the resident Microsoft® certificate Server software package or remotely by VeriSign™ OnSite service. Windows NT and IIS permit a certificate to be mapped to a system account to further define the level of access assigned to each user down to the file level.

14. SUBJECT TERMS
IT-21, Microsoft Windows NT, Microsoft Internet Information Server, Certificates

15. NUMBER OF PAGES
114

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFI- CATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

Approved for public release; distribution is unlimited

IT-21 COMPLIANT CONTROLLED ACCESS TO INTERNET WEB PAGES

Marcia S. Sonon
Lieutenant, United States Navy
B.S., Purdue University, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL

September 1998

Author: _____

Marcia S. Sonon

Approved by: _____

Gus K. Lott, Thesis Advisor

_____

Daniel F. Warren, Second Reader

_____

Dan C. Boger, Dean
Computer and Information Science and Operations

ABSTRACT

Although numerous resources are available to achieve Internet presence by creating and publishing a web site, security and access control within the site are very limited. The Navy's support of the IT-21 initiative embracing the Microsoft® Windows NT® operating system (OS) provides solutions to not only restrict entry to the site, but also to control access to content on the web page.

Work detailed in this thesis addresses the issue of security by exploring the Windows NT OS and activating its inherent security features to protect the overall system from intrusion and attacks from the Internet. The web pages are published using Microsoft® Internet Information Server 4.0 (IIS) and FrontPage™ 98. Access is controlled by issuing certificates from the resident Microsoft® certificate Server software package or remotely by VeriSign™ OnSite service. Windows NT and IIS permit a certificate to be mapped to a system account to further define the level of access assigned to each user down to the file level.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

ACL	Access Control List
ActiveX	A technology developed by Microsoft for sharing information among different applications
ADO	ActiveX Data Objects
API	Application Programming Interface
ASP	Active Server Page
ATM	Asynchronous Transfer Mode
AUTODIN	Automatic Digital Network: Current Department of Defense messaging system
C2	Class 2
C4I	Command, Control, Communications, Computers, and Intelligence
CA	Certificate Authority
CD-ROM	Compact Disc Read-Only Memory
CGI	Common Gateway Interface
CINCPACFLT	Commander in Chief, Pacific Fleet
CISC	Complex Instruction Set Computer
COE	Common Operating Environment
COTS	Commercial Off-The-Shelf
CPU	Central Processing Unit
CRL	Certificate Revocation List
DAC	Discretionary Access Control
DCOM	Distributed Component Object Model
DII COE	Defense Information Infrastructure Common Operating Environment
DLL	Dynamic Link Library
DOD	Department of Defense
e-mail	Electronic Mail
EDO	Extended Data Out (a memory configuration for fast Pentium)
EIDE	Extended Integrated Device Electronics
ERD	Emergency Repair Disk
FAT	File Allocation Table
Fiber	Fiber Optic Cable
FTP	File Transfer Protocol
GB	Gigabyte
GIF	CompuServe Graphics Interchange Format for images
HAL	Hardware Abstraction Layer
HTML	Hypertext Markup Language
HTTP	Hypertext Transport Protocol

IDE	Integrated Drive Electronics
IIS	Internet Information Server
INFOSEC	Information Security
ISAPI	Internet Server Application Programming Interface
ISM	Internet Service Manager
ISP	Internet Service Provider
IT-21	Information Technology for the 21st Century
ITSEC	Information Technology Security Evaluation Criteria (UK)
ITU	International Telecommunication Union
JPEG	Joint Photographic Experts Group compressed file image format
JTA	Joint Technical Architecture
KB	Kilobyte
LAN	Local Area Network
LPC	Local Procedure Call
LSA	Local Security Authority
MAN	Metropolitan Area Network
MB	Megabyte
Mbps	Megabits per second; used to describe data transfer capacity
MHz	Megahertz
MIME	Multipurpose Internet Mail Extensions
MMC	Microsoft Management Console
NCSC	National Computer Security Center
NIC	Network Interface Card
NT	New Technology; full operating system name: Microsoft Windows NT
NTFS	NT File System
OC-3	Optical Carrier-3
ODBC	Open Database Connectivity
OEM	Original Equipment Manufacturer
OS	Operating System
OS/2	Operating System 2; an operating system designed by IBM
OSI	Open Systems Interconnection
PC	Personal Computer
PCI	Peripheral Component Interconnect
PCMCIA	Personal Computer Memory Card International Association
PCT	Private Communications Technology
PKCS	Public Key Cryptography Standards
PIN	Personal identification Number
POSIX	Portable Operating System Interface for UNIX

PPTP	Point-to-Point Tunneling Protocol
RAM	Random Access Memory
RDBMS	Relational Database Management System
RISC	Reduced Instruction Set Computer
ROM	Read-Only Memory
RPC	Remote Procedure Calls
SAM	Security Account Manager
SID	Security Identifier
S/MIME	Secure/Multipurpose Internet Mail Extensions
SQL	Structured Query Language
SRM	Security Reference Monitor
SSL	Secure Sockets Layer
SVGA	Super Video Graphics Array
TCP/IP	Transmission Control Protocol/Internet Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TWAIN	Technology Without Any Interested Name; a standard interface for scanners
UNIX	An operating system designed by AT&T Bell Laboratories
URL	Uniform Resource Locator
W3C	World Wide Web Consortium
WEC	Web Extender Client
WWW	World Wide Web
X.509	ITU-recommended certificate standard

I. INTRODUCTION

A. MOTIVATION

The Internet, or more specifically the World Wide Web multimedia portion familiar to the majority of users, has grown in popularity as a communication tool. Its features include a platform-independent means of conveying information, graphics, sound, files, etc.

The Web was developed in early 1989 by researchers at the European Laboratory for Particle Physics in Geneva, Switzerland. The goal was to create an online system that would allow nontechnical users to share data "online" without the need for remembering extensive commands or using complicated interfaces. Developers began designing and creating browsers that would simplify the access methods to the information. By 1993, these web browsers and graphic pages began to change the way users viewed the Internet and accessed required information.

By posting information on a web page, that information becomes available to anyone who can access that particular web page by means of its Uniform Resource Locator (URL) through the browser interface.

The free flow of information has rapidly changed how our society does business, researches topics of interest, and views the world in general. The availability provided by web pages offers 24 hour access and reduces the need for dedicated communication channels for support, updates, and required information.

The focus of this thesis is to use the availability provided by the Internet as an advantage to monitor a remote system without the additional investment of dedicated communications equipment. The system can be monitored and even adjusted through links provided on a web page, thus requiring a limited amount of equipment to connect the remote system to the Internet. Access to the web page content can be achieved in various ways, including passwords, biometric interfaces at the user's site, and digital certificates to name a few. This implementation limits the access of most of the web page content to authenticated users identified by means of digital certificates.

With the introduction of the Navy's Information Technology for the 21st Century (IT-21) concept, new implementation standards are being instituted. IT-21 calls for PC-based tactical information network supported by Microsoft® Windows NT® servers and clients. The push to standardize the information infrastructure stems from a desire for improved information flow to the warfighter. The system used for this project consists of a digital still camera connected to a personal computer (PC), with Windows NT Server 4.0 as the operating system, to broadcast the images to the world.

Currently, most Internet services at NPS are provided by UNIX platforms. The goal of this project is to present an alternative solution using IT-21 compliant software and hardware not only to publish and administer a Web site, but also control user access.

B. SUMMARY OF CHAPTERS

Chapter II provides an overview of the IT-21 concept including the proposed standards for compliant software, hardware, and workstations. Since IT-21 calls for the

use of the Windows NT operating system (OS), Chapter III presents an in depth look at the Windows NT OS with an emphasis on the inherent security features and the steps required to meet Department of Defense C2 compliance. Chapter IV analyses Microsoft® Internet Information Server 4.0 and FrontPage 98, two key software applications necessary to publish and administer web pages in a Windows NT-based environment. Chapter IV examines access control using digital certificates to identify a user to the system, which also determines the amount of access granted to that individual. Chapter VI details the specifications of all hardware used for the project. Chapter VII states conclusions formulated through the work of this thesis and presents recommendations for the direction of future efforts.

Appendix A provides detailed permission changes for both the registry and files or directories for use with the Microsoft C2 Configuration Manger. Appendix B lists the recommendations for configuration of user rights on Navy systems.

II. IT-21 OVERVIEW

A. CHAPTER OVERVIEW

This chapter provides an overview of the Information Technology for the 21st Century (IT-21) concept. The minimum implementation standards for acquiring software, hardware and workstations for the U.S. Atlantic and Pacific fleet units and bases are presented.

B. IT-21 ORIGINS

Information superiority is the foundation of Joint Vision 2010 battlefield dominance. Each service in the Department of Defense (DOD) has a warfighting vision based on gaining and maintaining that information superiority. The shift in focus from platform-centric warfare to network-centric warfare throughout the military does not require merely the acquisition of new technology. It requires a plan to change the mindset of warfighters, to modernize and standardize the Navy's Command, Control, Communications, Computers and Intelligence (C4I) infrastructure, and to improve accurate and timely information dissemination to dispersed forces.

The IT-21 concept was originated by Admiral Archie Clemins, Commander in Chief, U.S. Pacific Fleet (CINCPACFLT). IT-21 is a coordinated networking initiative being implemented as a team effort between the Secretary of the Navy, Office of the Chief of Naval Operations, U.S. Atlantic and Pacific Fleets, the Space and Naval Warfare Systems Command, and the Naval Computer and Telecommunications Command. IT-21

strives to accelerate the transition from existing C4I programs to a personal computer (PC) based tactical warfighting network. The four elements of IT-21 are shipboard networks, commercial wideband satellite communications, shore-based infrastructure, and tactical and nontactical applications.

Guidance for absolute minimum standards and guidelines is provided by the Joint Technical Architecture (JTA) and Defense Information Infrastructure Common Operating Environment (DII COE). The office of the Department of the Navy Chief Information Officer has published the Information Technology Standards Guidance version 98-1.1 to provide guidance for standardizing information systems. The initial release of this document can be found at [http://www.doncio.navy.mil/itsgpublic]. The ultimate goal is to link communication between all U.S. forces and eventually link allies as well. The emphasis is on exchanging classified and unclassified, tactical and non-tactical information from a desktop computer.

In an era of continuing force reductions and budget cuts, IT-21 provides adaptable hardware and software implementation standards for fleet information systems. This approach adopts industry standards and advocates the use of commercial off-the-shelf (COTS) technology in a client-server environment allowing the user to pull just what information is needed in a seamless manner [Ref. 1]. The fleets cannot afford to continue support for diverse operating systems (OS) that require separate training, operational procedures, troubleshooting requirements for interoperability between operating systems, and maintenance in a time of shrinking defense budgets.

The goal of driving all information gathering resources to a single PC allows multiple functions on a single workstation instead of multiple workstations dedicated to single function. This will reduce the number of workstations required, reduce the shipboard space needed, and increase productivity of the individual warfighter.

C. IT-21 STANDARDS

IT-21 standards represent current market technology in software, hardware, and workstation capabilities. The standards are dynamic in nature, and will adapt to keep pace with commercial trends.

1. Software Standards

Table 2.1 lists the minimum software standards introduced in a Message from CINCPACFLT in Reference 2, which will be updated periodically. All non-standard OS and electronic mail (e-mail) products will be replaced no later than December 1999 in anticipation of the inactivation of the current DOD messaging system (AUTODIN). There will be exceptions made in rare cases where there is an overwhelming reason to use a high-end UNIX workstation, such as application servers. Windows NT is the preferred operating system. When Windows NT is not practical, operating systems chosen must be standards based, primarily those that comply with X/Open CAE and Institute of Electrical and Electronics Engineers' (IEEE's) POSIX specifications. The guidance for personal workstations is to use operating systems that comply with Win 32 standard interfaces for long-term usability.

All relational databases capable of supporting World Wide Web (WWW) technology in accordance with COE will be used to support data requirements and application development. Relational database management systems (RDBMS) software that support web technology include Oracle®, Sybase® SQL Server™, Microsoft® SQL Server, and Microsoft® Access.

Software Category	IT-21 Minimum Standard
Operating System	Microsoft® Windows NT® 4.0/5.0 Server Microsoft® Windows NT® 4.0/5.0 Workstation
Electronic Mail	Microsoft® Exchange 5.0
Office Software	Microsoft® Office 97 Professional
Anti-Virus Protection	IBM® AntiVirus
Additional Software	Microsoft® BackOffice™ Client, Microsoft® Outlook 97, Microsoft® Image Composer

Table 2.1 IT-21 Minimum Software Standards [Ref. 2]

2. Hardware Standards

Table 2.2 lists the minimum network hardware standards, and Table 2.3 on the following page lists the minimum workstation standards introduced in Reference 2. Since software requirements drive hardware standards, these standards will be upgraded in response to commercial trends and new technological advances.

D. CHAPTER SUMMARY

In general, IT-21 is an effort to improve the flow of information by concentrating funding and training on industry-standard software, hardware, and workstations. The emphasis is on bringing the power of timely, accurate information to the warfighter in the field or afloat. The minimum standards for acquiring software, hardware and workstations set a foundation for future growth that ensures interoperability between Navy information systems. It is the proposed IT-21 standards for workstations and software that determined the type of hardware purchased for this project, the software products chosen for implementation of the Web site, and the type of access control used.

Hardware Category	IT-21 Minimum Standard
Afloat LANs	ATM Fiber backbone, 100 Mbps (Fast Ethernet) to PC
Ashore Tactical and Headquarters Command Centers	ATM Fiber backbone, 100 Mbps (Fast Ethernet) to PC
Ashore Tactical Support Command	ATM Fiber backbone, 100 Mbps (Fast Ethernet) to PC
Metropolitan Area Networks (MAN)	Capable of at least OC-3 (155 Mbps)

Table 2.2 IT-21 Minimum Hardware Standards [Ref. 2]

Workstation Type	IT-21 Minimum Standard
PC Capabilities	200 MHz Pentium Pro CPU 64 MB EDO RAM 3.0 GB Hard Disk Drive 3.5 inch Floppy Disk Drive 8X IDE CD-ROM Dual PCMCIA/PC Card Reader PCI Video Card with 2 MB RAM 17 inch Monitor (1280 x 1024) Pointing Device (Trackball or Mouse) Soundblaster (Compatible) Audio Card with Speakers Keyboard CPU Compatible with 100 Mbps Fast Ethernet NIC
Laptop Capabilities	Dual 150 MHz Pentium CPU 32 MB EDO RAM 2.1 GB EIDE Hard Disk Drive 6X Internal CD-ROM PCMCIA Slots Modem or Network Interface Card (NIC) 12 inch SVGA Active Matrix Color Display Smart Lithium Battery

Table 2.3 IT-21 Minimum Workstation Standards [Ref. 2]

III. WINDOWS NT SERVER

A. CHAPTER OVERVIEW

This chapter provides background information regarding the development of Microsoft® Windows NT® and a look at the design goals and implementation of a Windows NT Server. The security aspects of Windows NT are presented as they pertain to the security subsystem, the use of service packs to correct deficiencies and add enhancements, a brief overview of the U.S. government C2 requirements, and how Windows NT fulfills the requirements with the implementation of the C2 Configuration Manager and some additional modifications.

B. HISTORY OF WINDOWS NT

The Microsoft Windows NT development team was formed in 1989. The team mission was defined as:

> To design and build a personal computer operating system that would meet the current and future operating system needs of the PC platform [Ref. 3].

To accomplish the mission, the following market requirements were identified:

- To provide easy portability to other 32-bit architectures
- To provide scalability and multiprocessing support
- To support distributed computing, allowing multiple computers to share resources
- To support the application programming interfaces (APIs) required by the Portable Operating System Interface for UNIX (POSIX)
- To provide U.S. Government Class 2 (C2) security features, and to provide a path to Class B1 and beyond

Microsoft's design team prioritized goals, including robustness, extensibility and maintainability, portability, performance, POSIX compliance, and government certifiable C2 security. For robustness, the operating system should actively protect itself from internal malfunction and external damage. It must respond predictably to software and hardware errors. The NT system must be straightforward in its architecture and coding practices, and interfaces and behavior be well specified. For extensibility and maintainability, the OS must be designed to grow and adapt to future needs of Microsoft and the original equipment manufacturers (OEMs).

The system must accommodate changes and additions to the API sets supported. In addition, the APIs should not employ flags or other devices to drastically alter functionality. By using subsystems to implement major portions of the system, Windows NT can isolate and control dependencies. [Ref. 3]

The system architecture must be portable to a number of other platforms with minimal recoding. The design must include algorithms and data structures that produce a high level of performance and provide the flexibility needed to achieve the performance goals. Finally, the goal for the POSIX standard calls for operating system vendors to implement UNIX-style interfaces so that applications can be moved easily from one system to another. U.S. government security guidelines specify certain protections such as auditing capabilities, access detection, per-user resource quotas, and resource protection. [Ref. 3]

C. WINDOWS NT DESIGN

The Windows NT system design consists of:

- executive
- internal processes
- a set of non-privileged servers called protected subsystems

The executive runs in kernel—or privileged processor—mode providing system services. The executive serves as the only entry point into the system. The protected subsystems run in non-privileged—or user—mode outside of the executive. A protected subsystem executes in user mode as a regular process. The subsystem may have extended privileges as compared to an application, but it is not considered a part of the executive and cannot bypass the system security architecture or corrupt the system in any other way. Subsystems communicate with their clients and each other using local procedure calls (LPCs).

The NT executive includes a set of system service components—the Object Manager, the Security Reference Monitor, the Process Manager, and so forth—which are exposed through a set of system services similar to APIs. The executive performs some internal routines, but its primary responsibility is taking an existing process thread from a requesting subsystem or application, validate that the thread should be processed, execute it, and then return control of the thread to the requestor. Figure 3.1 displays the Windows NT 4.0 operating system basic architecture [Ref. 3]

The division of the OS into kernel-mode system services and subsystems adds a layer of validation to ensure improper application behavior will not crash the operating

system. In addition, each service is required to capture and probe the values of any arguments upon which it will operate to ensure that the caller or one of its threads cannot dynamically alter the value or delete the memory in which it is contained. Most arguments do not need explicit capture if they are passed in registers and arguments passed in memory are probed and captured by the system service dispatcher as necessary. Address-space layout includes both user address space and system address space. In order to maintain separation, a 64 KB boundary is included which is inaccessible to both user and system modes. [Ref. 3].

Most of NT's code is written in C language, but some of its modules are written in C++ and Assembly. All the system's code dependent upon the hardware is isolated into a library called the Hardware Abstraction Layer (HAL). The HAL enables Windows NT to be very portable, allowing adaptation to both RISC (Reduced Instruction Set Computer) and CISC (Complex Instruction Set Computer) hardware platforms. Since it is a true 32-bit multitasking OS, NT 4.0 allows you to run programs totally independent from each other in their own separate memory space [Ref. 4]

Windows NT Server support of communication and internetworking features includes Distributed Component Object Model (DCOM) for distributed applications; Point-to-Point Tunneling Protocol (PPTP) to create secure private intranets over the Internet; and MultiProtocol Router to provide Local Area Network (LAN) to LAN routing of TCP/IP, IPX, and AppleTalk protocols.

D. SECURITY

This section will outline the features of Windows NT 4.0 security subsystem and recommended changes to the default system configuration to improve security.

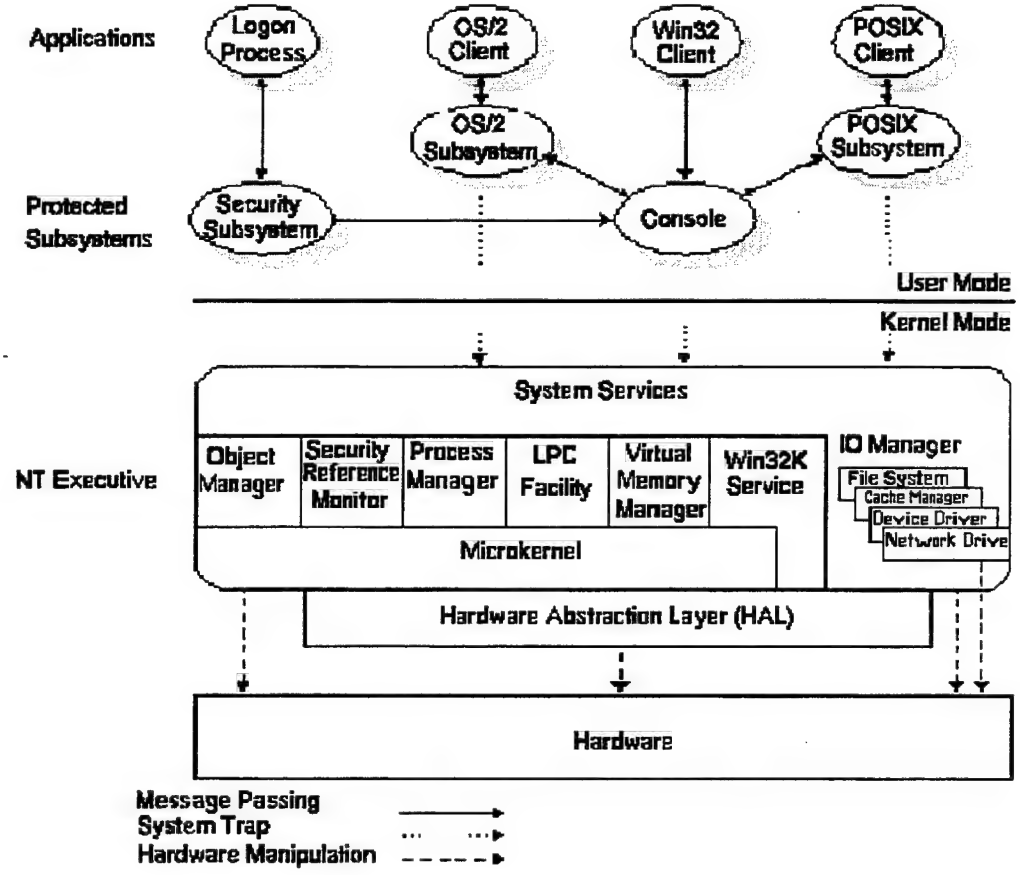

Figure 3.1 Windows NT 4.0 Basic Architecture [Ref. 3]

1. Security Subsystem

The NT security architecture provides a secure means to control all access to objects. The NT OS represents virtually everything as an object including memory devices, system processes, threads, and windows appearing on the desktop. An object is

a self-contained entity maintaining its own data and functions required to manipulate the data, including who or what processes can access that data or resources. Access to objects is regulated by the security subsystem to ensure access is only granted with proper authorization. An administrator is able to assign permissions to users or groups to grant or deny access to specific objects.

The Logon Process protected subsystem, Security protected subsystem, and the Security Reference Monitor (SRM) form the security model for Windows NT. The security subsystem is comprised of the Local Security Authority (LSA) and Security Account Manager (SAM) which work in conjunction with the Security Reference Monitor and the logon processes.

a. Security Identifiers

A unique Security Identifier (SID) instead of a username identifies Windows NT users to the system. The security subsystem generates a SID when the account is created using a proprietary hashing function. The hashing function to create the SID is based on the current system time, the amount of user-mode execution time for the current process, and the computer name or domain name. A SID cannot be reused, even if the same user account name is reinstated. In the case where an account is removed and then recreated, a new SID will be created. If the user belongs to a group, a unique SID for that group will be created while the user maintains his or her own unique SID. [Ref. 5]

b. Local Security Authority (LSA)

The Local Security Authority serves as the central component of the security subsystem with the responsibility of generating access tokens, managing security policies on the local computer, and facilitates user logon authentication. [Ref. 5] As soon as the SAM verifies the password against the user database, the LSA creates an access token for that user that includes the unique SID and user privileges. The user, and every process he or she starts, is associated with that access token. When a user tries to access a secured object, his or her access token is checked against the object's ACL. Whenever a user wishes to do something that is associated with a privilege, the security subsystem examines the access token.

c. Security Account Manager (SAM)

The Security Account Manager maintains the security accounts database of all local user and group account information, including domain accounts when in NT Server mode. The SAM verifies and identifies users during the logon process by comparing user-entered data to authentication data—such as passwords—from its database. The SAM provides the SID when requested by the LSA at logon for user validation. [Ref. 4]

d. Security Reference Monitor (SRM)

Serving as the enforcer for the security subsystem, the Security Reference Monitor prevents direct access to objects by users and processes lacking proper permissions. The SRM is fixed in kernel mode and provides services to check user

access rights at each request. Information regarding success or failure of user access attempts and any necessary audit messages are sent to the LSA to be logged. The SRM responds to both user and system authorization requests. [Ref. 5]

e. Access Control List (ACL)

An Access Control List is a directory of the sets of attributes associated with an object and the users—identified by SIDs—who may execute those attributes. The list of attributes and users is represented in a structure known as an Access Control Entry (ACE). Each ACE records access or auditing permissions to an object for a single user or group. For each object, there exist two associated ACLs. The Discretionary ACL represents rights that may be assigned by designated users and the System ACL, which is set by system security policies. [Ref. 5]

2. Service Packs

A service pack is a periodic update to the operating system that contains fixes to problems uncovered by users and enhancements to the OS. Since its introduction until August 1998, Microsoft has released three service packs for Windows NT 4.0.

Interim updates addressing specific problems are called hotfixes. Service packs are cumulative in that they include all fixes from previous service packs and new hotfixes. Hotfixes shall be installed in ascending order of date/time stamp on the executables, as some hotfixes will write over files modified by other hotfixes. A complete list of available service packs and hotfixes is available at ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3. Any

time new software or hardware components are installed, Service Pack 3 and current hotfixes must be reapplied. [Ref. 5]

3. C2 Security Measures

The original Windows NT design goal envisioned an OS capable of Class 2 (C2) level of trust according to the Department of Defense. In August 1995, the C2 rating was granted for Windows NT version 3.5 under the following conditions:

- U.S. Service Pack 3 for Windows NT 3.5 installed
- Server in a stand-alone configuration
- No network services enabled [Ref. 6]

In addition, Windows NT is under evaluation for its networking component of a secure system in compliance with the NCSC's "Red Book"—an interpretation of the Orange Book applied to network security. [Ref. 7] The UK Information Technology Security Evaluation and Certification (ITSEC) has given Windows NT an FC2/E3 rating—the equivalent of the C2 Red Book evaluation in the United States. [Ref. 4] This does not mean that Windows NT is C2 certified; no operating system is ever C2 certified. Certification applies to a particular installation, including hardware, software, and the system environment.

a. Definition of C2

The National Computer Security Center (NCSC) is a division of the National Security Agency and Department of Defense. Under presidential directive, NCSC is responsible for establishing policy and procedures for securing information valuable to the U.S. government. In order to help formalize the process of providing

adequate trust and assurance, the NCSC published a series of computer security guides detailing the requirements for various levels of trust in information systems.

Theses security guides are often referred to as the "Rainbow Series" after the colors used for the covers of the guides. The most popular book, originally titled *Trusted Computer System Evaluation Criteria* (TCSEC), is well known as the "Orange Book" due to the original color of its cover. First issued in 1983 and updated in December 1985, the TCSEC establishes a basis for evaluating operating system security. It has also been issued as a DOD standard, DOD 5200.28-STD. [Ref. 8]

C2-level security is referred to as Controlled Access Protection. [Ref. 9] Features of C2 systems include the accountability of users, discretionary controls, auditing, protect against resource (object) reuse, prevention of external tampering with system files in memory or on disk.

The operating system is required to clearly identify each individual user in order to distinguish between actions of different users. NT usually accomplishes this through the mandatory logon process using password controls.

Discretionary Access Control (DAC) is an access policy that restricts access to system objects—files, directories, and devices—based on the identity of a user or a group. DAC allows the owner or creator of an object to define access permissions to an object and the type of access allowed. A form of DAC uses ACLs to limit access to a resource to the degree of including or excluding single users. Windows NT fulfills this

requirement through its object access methodology of user and system permissions and ACLs [Ref. 5].

The operating system must track and record security-related events of all users in the system. This audit trail must be protected from modification or unauthorized access. Administrators on a Windows NT system are able to audit user and system events through the LSA logging process and by limiting access to the security log to only administrators. [Ref. 8]

Object reuse requirements protect files, memory, and other objects in a trusted system from being accessed accidentally by unauthorized users. The OS ordinary access control features determine appropriate access to objects assigned to specific users. Object reuse requirements address what happens when these objects are reassigned. These requirements must ensure the object being assigned, allocated or reallocated does not contain data left over from previous users. [Ref. 9] Windows NT meets this criterion by clearing memory upon allocation to a process, removing pointers to a resource immediately after it is freed by the process, and disallowing the recovery of information contained in disk clusters that have been freed by other users.

Finally, the OS must be protected against external tampering with system files in memory or on disk. Windows NT enforces this requirement through memory and disk space barriers such as separation of user memory space and system memory space and the use of ACLs for memory and disk objects.

Figure 3.2 provides a graphical representation of requirements for TCSEC evaluation.

Trusted Computer System Evaluation Criteria Summary Chart

	D	C1	C2	B1	B2	B3	A1
Security Policy							
Discretionary Access Control		⊗	⊗	⇒	⇒	⊗	⇒
Object Reuse			⊗	⇒	⇒	⇒	⇒
Labels				⊗	⊗	⇒	⇒
Label Integrity				⊗	⇒	⇒	⇒
Exportation of Labeled Information				⊗	⇒	⇒	⇒
Labeling Human Readable Output				⊗	⇒	⇒	⇒
Mandatory Access Control				⊗	⊗	⇒	⇒
Subject Sensitivity Labels					⊗	⇒	⇒
Device Labels					⊗	⇒	⇒
Accountability							
Identification and Authentication		⊗	⊗	⊗	⇒	⇒	⇒
Audit			⊗	⊗	⊗	⊗	⇒
Trusted Path					⊗	⊗	⇒
Assurance							
System Architecture		⊗	⊗	⊗	⊗	⊗	⇒
System Integrity		⊗	⇒	⇒	⇒	⇒	⇒
Security Testing		⊗	⊗	⊗	⊗	⊗	⊗
Design Specification and Verification				⊗	⊗	⊗	⊗
Covert Channel Analysis					⊗	⊗	⊗
Trusted Facility Management					⊗	⊗	⇒
Configuration Management					⊗	⇒	⊗
Trusted Recovery						⊗	⇒
Trusted Distribution							⊗
Documentation							
Security Features User's Guide		⊗	⇒	⇒	⇒	⇒	⇒
Trusted Facility Manual		⊗	⊗	⊗	⊗	⊗	⇒
Test Documentation		⊗	⇒	⇒	⊗	⇒	⊗
Design Documentation		⊗	⇒	⊗	⊗	⊗	⊗

⊗ New or enhanced requirements for this class

⇒ No additional requirements for this class

(blank) No requirements for this class

Figure 3.2 TCSEC Evaluation Requirements [After Ref. 9]

b. Microsoft C2 Configuration Manger

The default Windows NT 4.0 installation does not provide adequate security to be considered C2 compliant, even with Service Pack 3 and all recommended post service pack fixes installed. Additionally, any NT system connected to any type of network will not be considered C2 compliant. An NT 4.0 system can be manually configured for C2 compliance; however, the Microsoft® Windows NT® Server Resource Kit includes useful administration tools such as the C2 Configuration Manager to automate the process of configuring the OS.

The C2 Configuration Manger provides a graphical representation to indicate the current state of each required and recommended security feature. Figure 3.3 displays the configuration interface, which represents a system configured to be C2 compliant except for the networking services.

Dark red padlocks indicate items that are required for C2 compliance. Light blue padlocks indicate recommended items that are not required for C2 compliance. A closed padlock indicates an item is secured; in the case of a red padlock, the item is secured to be C2 compliant. An open padlock is a feature that has not been secured and is a possible security risk. A question mark indicates the C2 Configuration Manager could not determine the settings. A brief description follows of the system changes effected by each feature when selected for C2 compliance.

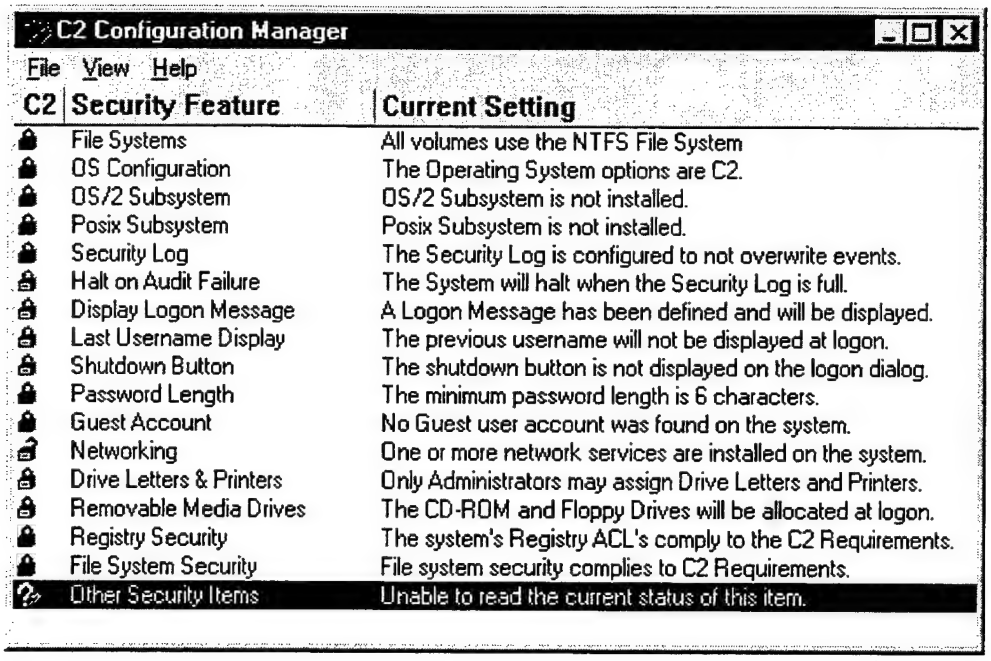

Figure 3.3 C2 Configuration Manager Graphical Interface [Ref. 10]

"Convert all File Systems to NTFS" will convert all disk volumes to the NT File System (NTFS). Under Windows NT, only NTFS supports DAC to the files and directories for secure access to the files. The File Allocation Table (FAT) used for file system indexing until the introduction of Windows 95 lacks access controls for permissions at the file level. FAT cannot be used for memory volumes greater than 2 GB. In addition, NTFS allows for auditing system events, file compression, and supports journaling, which logs all system writes to undo failed writing operations with minimal file corruption.

"OS Configuration" sets the boot selection timeout to zero. To be C2 compliant, Windows NT must be the only operating system on the computer. With the boot.ini timeout set to zero, Windows NT will be the default OS.

"OS/2 Subsystem" removes the files OS2.exe and OS2SS.exe for the OS/2 subsystem. For C2 configuration, Windows NT must be the only OS on the computer. Although the executable files have been removed, the registry keys have not been removed.

"Posix Subsystem" removes the files PSXSS.exe for the POSIX subsystem. For C2 configuration, Windows NT must be the only OS on the computer. Although the executable files have been removed, the registry keys have not been removed.

"Security Log," when secured, requires that the security logs never overwrite events, despite the age of the events. This ensures that the security logs must be cleared manually by the administrator on a regular basis.

"Halt on Audit" forces the system to halt if events cannot be written to the security log due to lack of available memory for the log. If the system halts due to a full security log, an administrator must restart the system and clear the log. Failure to clear the security log on a regular basis could result in denial of service.

"Display Logon Message" is not a C2 requirement; however, it is recommended that systems display a warning message before logon to indicate the private nature of the system. The Navy uses a standard warning banner that can be downloaded from the United States Navy Information Security (INFOSEC) Web Site Server at [http://infosec.nosc.mil/infosec.html]. This warning banner informs users that

their actions can be monitored and they can be held legally liable for unauthorized use of system resources.

"Last Username Display" is not required for C2, but it is recommended that the NT default state allowing the previous username displayed on the logon window be changed. This will ensure that any user is unable to determine the previous user of the system in order to exploit the system.

"Shutdown Button" removes the option of shutting down the system from the logon window without logging on a Windows NT workstation. Disabling the feature is not a requirement for C2, but it permits only the administrators to determine which users are authorized to perform system shutdowns.

"Password Length" changes the password options to prohibit blank passwords. The C2 Configuration Manager sets the default minimum password length to six characters, but can be set to any number of characters appropriate for the security of the system.

"Guest Account" disables the default Guest account on the system. In Windows NT 4.0, the Guest account is disabled by default. Users must provide a valid username and password or other acceptable identification to gain access to the system.

"Networking" disables all network services and capabilities from the computer. The C2 configuration requires that all network services be removed for compliance.

"Drive Letters & Printers" may be assigned by any user by default. This feature is not required for C2, but it is recommended that only Administrators be allowed to assign these resources. The C2 Configuration Manager will assign these tasks to the Administrators Group when the Secure button is selected.

"Removable Media Drives" will only allow authorized interactive users to access files on floppy or CD-ROM drives. These drives are allocated to a user as part of the interactive logon process and deallocated when the user logs off.

"Registry Security" allows the C2 Configuration Manager to make changes to several registry keys; however, it does not secure the registry. The "Guide to Implementing Windows NT® in Secure Network Environments" [Ref. 5] includes a modified C2regacl.inf file in accordance with the guide. Each registry can also be modified manually applying the permission changes in Appendix A. Following changes to the registry, the registry editor should be set to "read-only" mode to prevent tampering. The system should be restarted twice, and a new Emergency Repair Disk (ERD) should be created to backup the recent registry changes.

"File System Security" allows the C2 Configuration Manager to make changes to file and directory permissions. The "Guide to Implementing Windows NT® in Secure Network Environments" [Ref. 5] includes a modified C2ntfacl.inf file in accordance with the guide. Appendix A contains a list of all recommended file and directory permissions that are changed by the C2 Configuration Manager by implementing the modified C2ntfacl.inf file from the "Secure Windows NT Installation

and Configuration Guide" [Ref. 11]. In addition, the DOS and os2 directories should be removed from the %SystemRoot%\system32 directory as well as the files: os2.exe, os2ss.exe, os2srv.exe, psxss.exe, posix.exe, and psxdll.dll.

Even a Windows NT 4.0 C2 configured system is still vulnerable to exploitation. Further steps are required. Figure 3.4 lists additional C2 requirements and other security considerations under "Other Security Items".

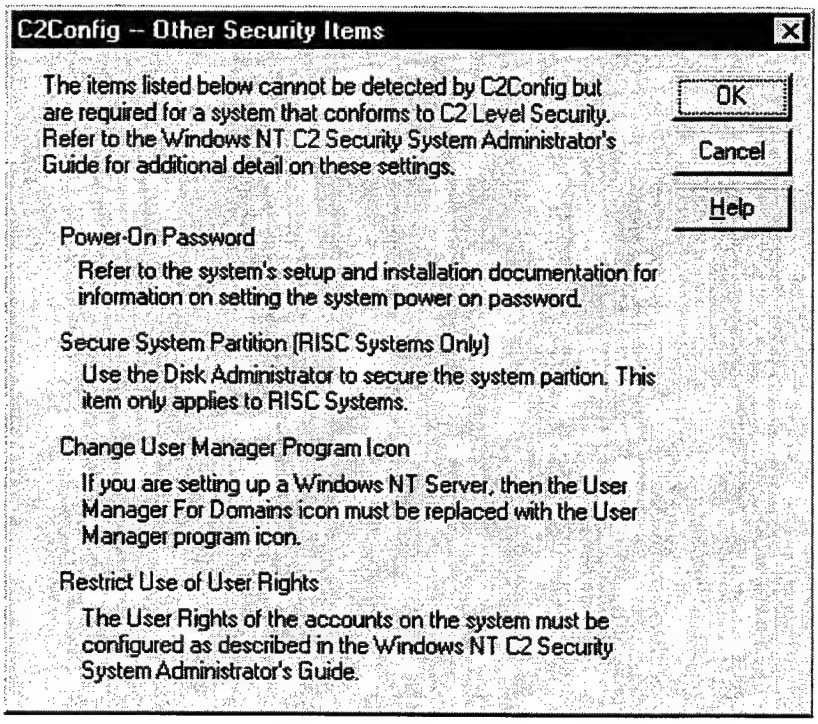

Figure 3.4 Additional Recommended Security Items [Ref. 10]

c. Instituting Account Policy

User account policies are used by the system to define password attributes and account lockout behavior. The Windows NT default account policies do not provide adequate security controls within a secure environment. The Microsoft® User Manager

for Domains provides an Account Policy dialog box divided into Password Restrictions and Account Lockout. Figure 3.5 illustrates the Account Policy dialog box including the recommended settings.

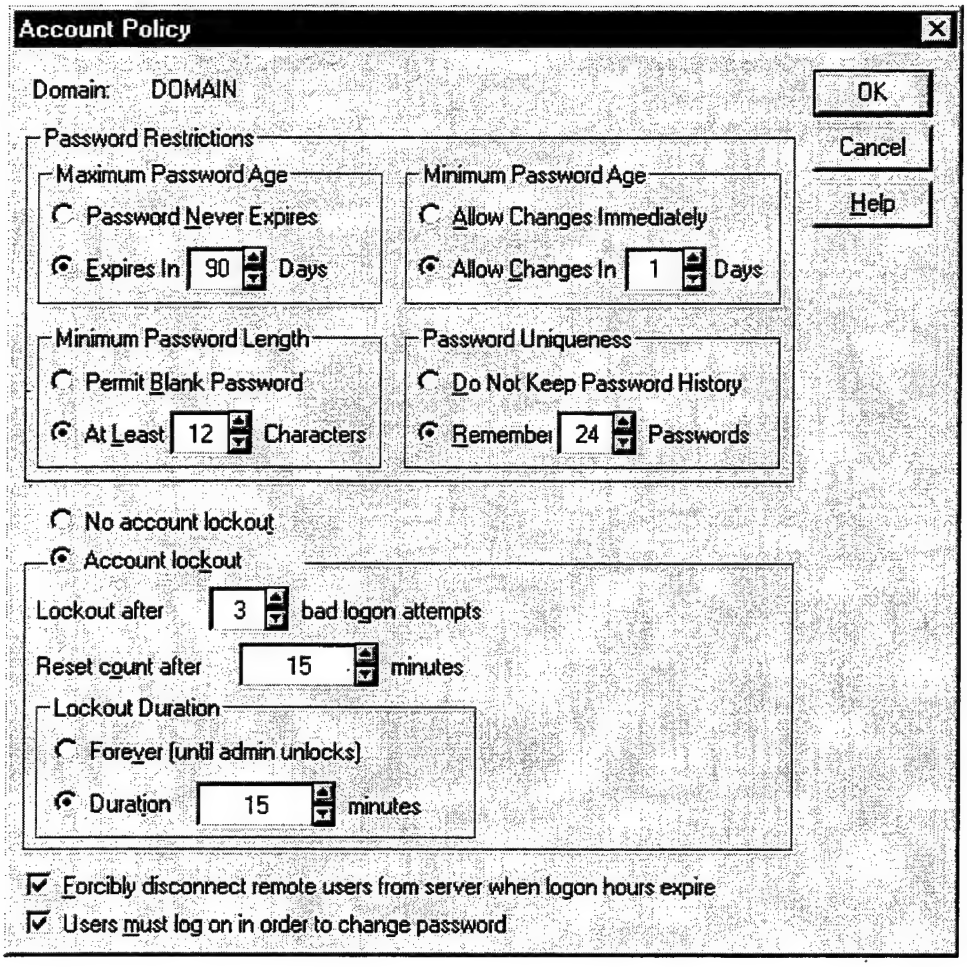

Figure 3.5 Account Policy Dialog Box [Ref. 12]

On Windows NT 4.0, strong password filtering can be used to enhance the account policy. Service Pack 3 includes a Dynamic Link Library file, passfilt.dll, which enforces strong password requirements for all users. Passfilt.dll should be used in place of fpnwclnt.dll unless it is essential for foreign account database synchronization.

Passfilt.dll implements a policy requiring passwords to be at least six (6) characters long, may not contain the user name or any part of the user's full name, and must contain characters from at least three of the following classes:

- English upper case letters (A, B, C, ...Z)
- English lower case letters (a, b, c, ...z)
- Westernized Arabic numerals (0, 1, 2, ...9)
- Non-alphanumeric (special characters such as punctuation marks) [Ref. 13]

d. Establishing User Rights

User rights define the allowable actions of users on a system in addition to the built-in allowable actions. The Windows NT default user rights do not provide adequate security controls within a secure environment. The Microsoft® User Manager for Domains provides a User Rights Policy dialog box to allow administration of standard and advanced user rights to strengthen the security of the Windows NT system. Both the "Guide to Implementing Windows NT® in Secure Network Environments" [Ref. 5] and "Securing Microsoft Windows NT Installation" [Ref. 7] provide detailed explanations of standard and advanced user rights options and include recommendations for changes depending upon the system configuration. "Securing Microsoft Windows NT Installation" [Ref. 7] user rights recommendations are located in Appendix B.

e. Auditing

The auditing feature of Windows NT allows administrators to track user accesses or modifications to files or directories. The audit log can be reviewed using the Event Viewer, which identifies potential security threats to the system. Audit logs must be archived and cleared on a regular basis to avoid denial of service due to memory

depletion. The permissions on a directory created for storing the archived logs must be changed to allow access by only administrators.

As an additional security measure, the archived event logs should be backed up, or permanently removed from the hard drive, to a data tape and physically secured. Figure 3.6 represents the recommended settings for an audit policy and Figure 3.7 displays the option for directory auditing.

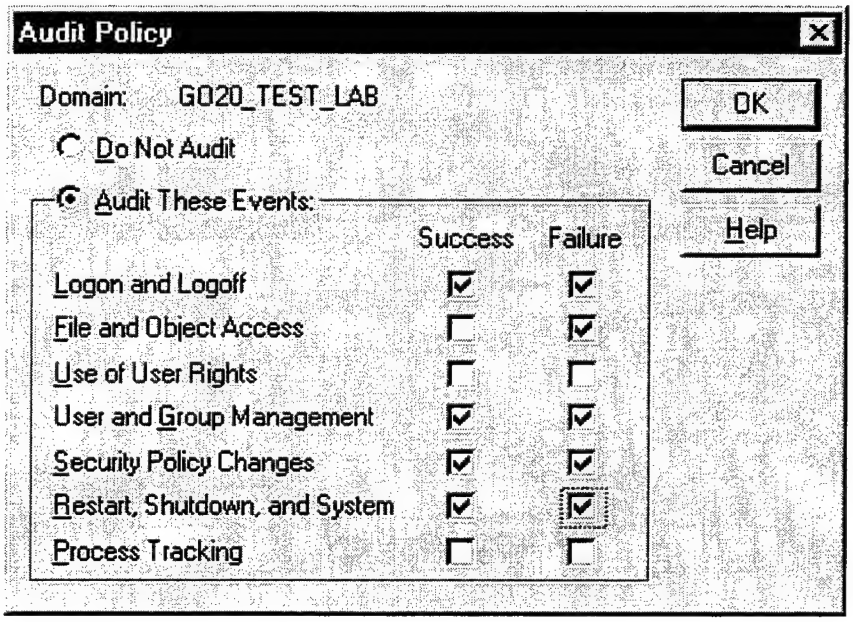

Figure 3.6 Recommended Audit Policy [Ref. 12]

E. CHAPTER SUMMARY

This chapter provides the background information required to understand the development of Microsoft® Windows NT® from the beginning design goals to the current implementation of Windows NT Server 4.0. The emphasis of this section is to first secure the platform before adding the needed software. The security features of

Windows NT are explained as they pertain to the interactions of the security subsystem and the use of service packs to correct deficiencies and add enhancements. A brief overview of the U.S. government C2 requirements is included as well as an examination of how Windows NT measures up to the requirements with the use of the C2 Configuration Manager and some additional modifications.

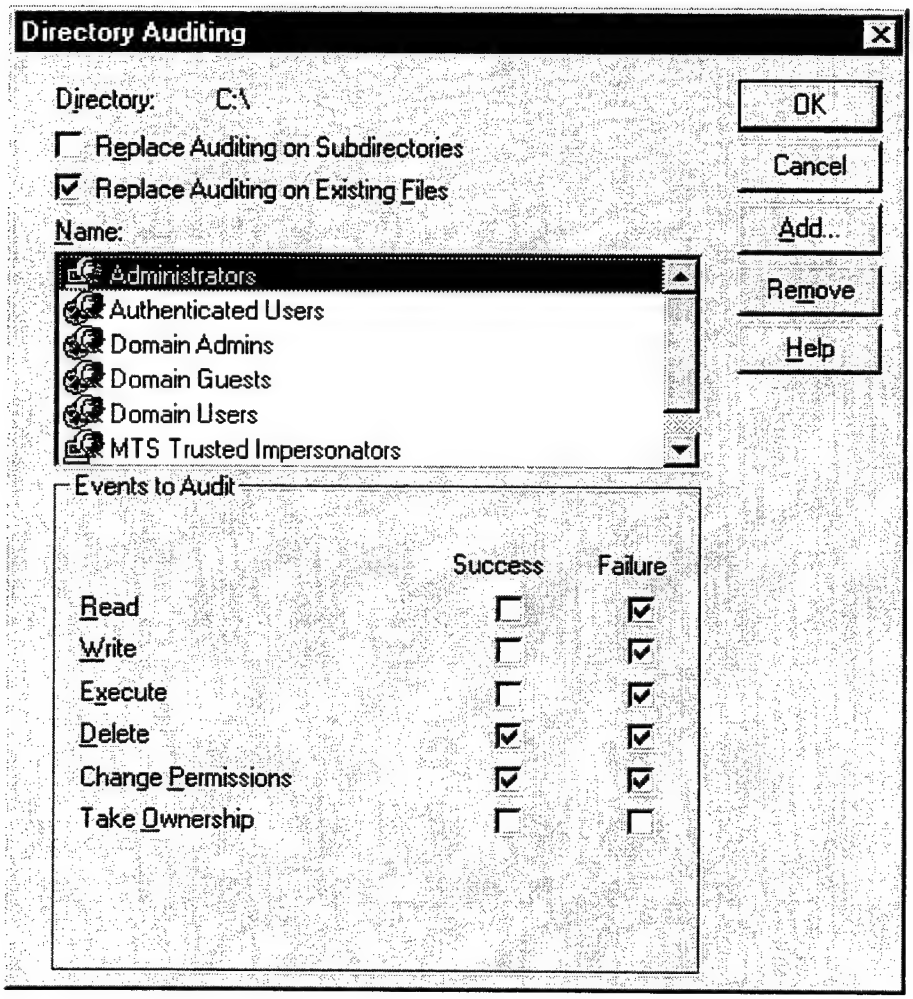

Figure 3.7 Directory Auditing

IV. SOFTWARE APPLICATIONS

A. CHAPTER OVERVIEW

This chapter focuses on the various software applications utilized throughout this project. The chapter begins by introducing the Microsoft® Internet Information Server 4.0 (IIS) and its integration with Windows NT to provide Internet services. Next, Microsoft® FrontPage® 98 is discussed.

B. MICROSOFT INTERNET INFORMATION SERVER

Microsoft Internet Information Server 4.0 is designed to enhance the World Wide Web capabilities of Windows NT Server 4.0 operating system. IIS 4.0 is available in the Windows NT 4.0 Option Pack, which does not usually come packaged with NT Server 4.0. IIS is designed for users who wish to have Web presence, whether a small business or an Internet Service Provider (ISP).

In order to provide support for Internet publishing, IIS consists of many components including transport services, client applications, administrative tools, database and applications connectivity to list a few. The major components comprising IIS 4.0 are:

- World Wide Web Service
- File Transfer Protocol (FTP) Service
- Gopher Service
- Internet Database Connector
- Secure Sockets Layer
- Internet Service Manager
- Browsers

The tight integration between Windows NT Server and IIS affords the ability to share applications and interfaces with NT services as well as utilizing administration tools. [Ref. 14] For example, IIS uses the same security accounts manager (SAM) as Windows NT Server to maintain users and groups to prevent multiple sets of network and Web site users. Also, IIS supports the Internet Server application programming interface (ISAPI) that is a platform and API allowing preprocessing and postprocessing of data stored on IIS. [Ref. 15]

Virtual directories are another highlight in IIS. Web administrators can assign virtual directories to distribute the physical storage of published information from multiple servers on the network to appear as a single directory structure to external clients

Graphical HTML editing can be accomplished without HTML programming knowledge by using new wizards and templates. Developers can also use languages with which they are already familiar to develop applications. Active Server Pages—a language-neutral scripting environment—provides a quick and efficient means for rapid application development. Java Virtual Machine is integrated to provide a reliable environment for running Java components on the server with Active Server Pages. Information may be published to the Web quickly and easily using a Web browser or the Web publishing wizard.

1. System Requirements

IIS 4.0 is designed for use with Microsoft Windows NT Server 4.0 with Service Pack 3 installed. Intel-based systems are recommended to have at least 90 MHz Pentium

processor, 32 to 64 MB RAM, and 200 MB hard disk space. DEC Alpha-based systems are recommended to have a 200 MHz processor, 64 MB RAM, and 200 MB hard disk space. Also, Microsoft Internet Explorer 4.01 is recommended for browsing capabilities.

2. World Wide Web Service

The WWW service is the heart of IIS. Hypertext Transfer Protocol (HTTP) is the application-level protocol used by the Web. IIS WWW Service performs the hypertext document publishing function for the Web server. It is powerful enough to host multiple Web sites on a single IP address with Browser-Neutral Host Header Support. Traditionally, each Web site would need to be hosted by its own installation of the Web service requiring the allocation of more server resources for redundant processes. This feature is referred to as Virtual Server support or Multi-Homing. The server can be configured to support multiple TCP/IP addresses.

3. FTP and Gopher Services

File Transfer Protocol (FTP) services allow users to transfer files between the FTP server and a client on a TCP/IP network. FTP offers the ability to copy files from as well as place files on the server. Not every site on the Internet is a graphical Web page and offers the ease of download scripts activated by clicking on an icon. FTP services allow access to reports, graphics, multimedia, and other information on Web pages, in data repositories, and archives that may or may not be published on the Web. Both DOS and Unix-style directory listings are supported. [Ref. 14]

Gopher is the name of a protocol used to search for and retrieve files from gopher servers on the Internet. The gopher service functions similar to FTP, but provides a menu-based user interface and allows a user to create hypertext links to other computers or services, annotate files and directories, and create custom menus. It is also referred to as a distributed document delivery system.

4. Internet Service Manager

Internet Service Manager (ISM) is run on the Windows NT Server or can be run in HTML format from a browser that supports frames and JavaScript for remote administration. The administration tool communicates by remote procedure calls (RPCs) that can be used either locally or remotely by any protocol that supports RPCs. The ISM for IIS 4.0 is implemented as a snap-in for the Microsoft Management Console (MMC). MMC is a common management console, which provides a consistent framework that can be used for all network administration programs. This framework integrates into a single console the tools, information, and views of the network required to perform an administrative task. The administrator can then use a console to manage the network, or provide a console to others to perform an administrative task. MMC does not by itself actually administer any part of the network, but displays consoles that host programs called *snap-ins*. The snap-ins, such as Internet Service Manger, User Manager and Key Manager, can be used to administer parts of the network from a single console.

Figure 4.1 displays a sample console for the Microsoft Management Console.

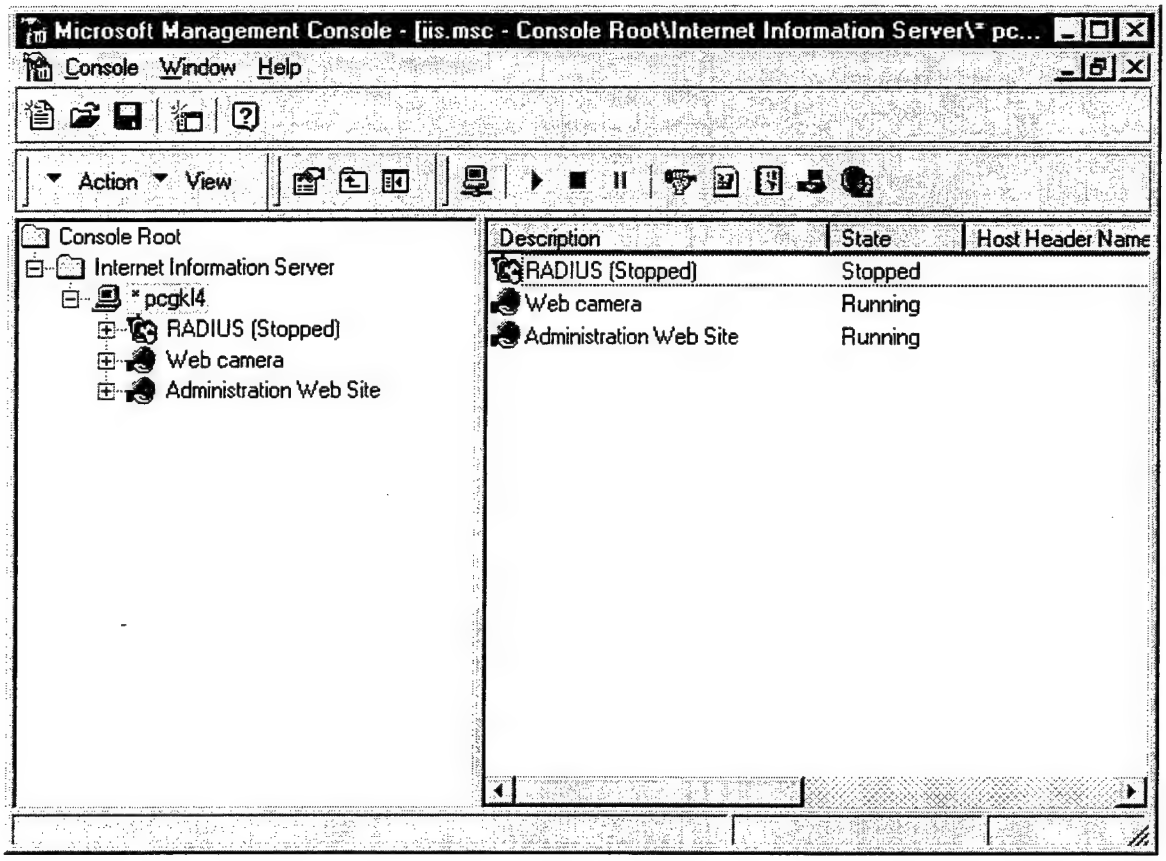

Figure 4.1 Microsoft Management Console

In addition, Bandwidth Throttling can be instituted to allocate network bandwidth for each Web site. Bandwidth Throttling will limit the amount of information that can be sent from the server at any one time. This ability offers the distribution of bandwidth among all services that share the server bandwidth access to resources. Therefore, one single Web page can not hoard all the bandwidth.

5. Security

User accounts and passwords must be protected, especially if the Internet server is compromised. User confidentiality can be protected by storing security information in an encrypted database on or off the server through an administrative domain structure.

The Secure Sockets Layer (SSL) component provides a security scheme for bulk-encrypting data between the server and its clients. In addition, administrators can limit the security context assigned to anonymous users in order to exercise control over the degree the server is exposed when connected to the Internet. Anonymous Internet logon permissions can be specified down to the file level.

a. Secure Communication

SSL is a public-key-based security protocol, introduced by Netscape, between the TCP and application layer (HTTP). The Microsoft equivalent technology is Private Communications Technology (PCT) and is compatible with SSL. For simplicity, all secure channels will be referred to as SSL.

SSL is application protocol independent in order to provide privacy and reliability between two communicating applications. The SSL Record Protocol—the lowest level—is layered on top of a reliable transport such as TCP. The Record Protocol is used for encapsulation of various higher level protocols. An example of an encapsulated protocol is the SSL Handshake Protocol that allows a server and client to authenticate each other, negotiate an encryption algorithm, and exchange cryptographic

keys before the application protocol begins to send to receive data. A higher level protocol can layer on top of the SSL Protocol transparently.

In order to take advantage of the security offered by SSL, the client needs to connect using SSL. This requires using HTTP with privacy (HTTPS) identifier in the URL, such as: [https://pcgkl4.ece.nps.navy.mil]. An initial handshake between server and client will define a secret key for the session to enable encrypted communications. Private key cryptography, such as DES or RC4, is used for data encryption. The client's identity can be authenticated using public key cryptography. Message transport under SSL includes a message integrity check. Web server performance will degrade due to the additional encryption; therefore, information that does not require a secure channel—such as image files—should remain as normal HTTP. There are additional encryption features in the Windows NT security model available to IIS.

b. File Access

Every potential user need not be recognized by the system in order to view Web page content. All requests for pages from IIS will first be accessed with IIS Anonymous User privileges. The Anonymous User is setup as a default when IIS is installed and creates a Windows NT account name IUSR_*machinename* on the Server. When enabled, IIS will first try to access requested pages as the Anonymous User by checking the file ACLs to see if it allows Anonymous User privileges. The file is only sent if the Anonymous User has sufficient privileges. The account is assigned as a member of the Guests Group with the ability to "Log On Locally." Access privileges are

checked for every file requested, not just the first file. Also, the user being authenticated anonymously does not have access to the password used in anonymous authentication. [Ref. 16]

IIS uses the NT security services for challenge/response authorization to access files if IUSR account permission is not granted. If the Web browser supports NT Challenge/Response, it will pass the user credentials to IIS. This provides authentication between the browser and the server without passwords being transmitted over the network. NT Challenge/Response requires a live connection between the Web client and the server requiring authentication. This is accomplished through a TCP/IP socket and will fail if the socket is lost or closed. If NT Challenge/Response fails, the Web browser requests Basic Authentication to pass user information to IIS. Basic authentication without SSL support will pass user information in the clear over the network and may allow the system to be compromised. [Ref. 16]

Web documents are retrieved from the Web server by the following process:

- The Web browser sends an HTTP Get Request to the Web server.
- The Web server evaluates the HTTP Get request and locates the document in question.
- The Web server attempts to open the document and finds that the file is restricted to certain users.
- The Web server then sends back an HTTP Response with the status 401 Unauthorized Access Denied. In the header, the Web server will indicate which means of authentication it accepts. The browser determines which method to use for authentication.

- If Basic authentication is being used, the user will then be prompted with a logon dialog box requesting user name and password. If NT Challenge/Response is in use the authentication will be performed without user interaction.
- The Web server uses this information to attempt to gain access to the requested file. If the user information provided has sufficient privileges, the Web server will continue to send the Web document from step 3. [Ref. 16]

Digital certificates can be issued by Microsoft® Certificate Server, which can be mapped to Windows NT user accounts to be used for authentication. IIS also allows for enhanced security based on IP addresses. IP security allows administrators to grant or deny access to an Internet service based on a TCP/IP address or group of addresses. [Ref. 14]

Figure 4.2 illustrates the flow of requests to the server.

c. Audit Logging Capabilities

IIS incorporates extensive logging capabilities. Log files can be automatically rotated based on the size of the log or by a specified time limit such as daily, weekly, or monthly. Information regarding services can be logged directly to an open database connectivity (ODBC) data source such as Microsoft SQL Server. It is recommended that audit logs or generated log reports be reviewed on a regular basis to detect security problems.

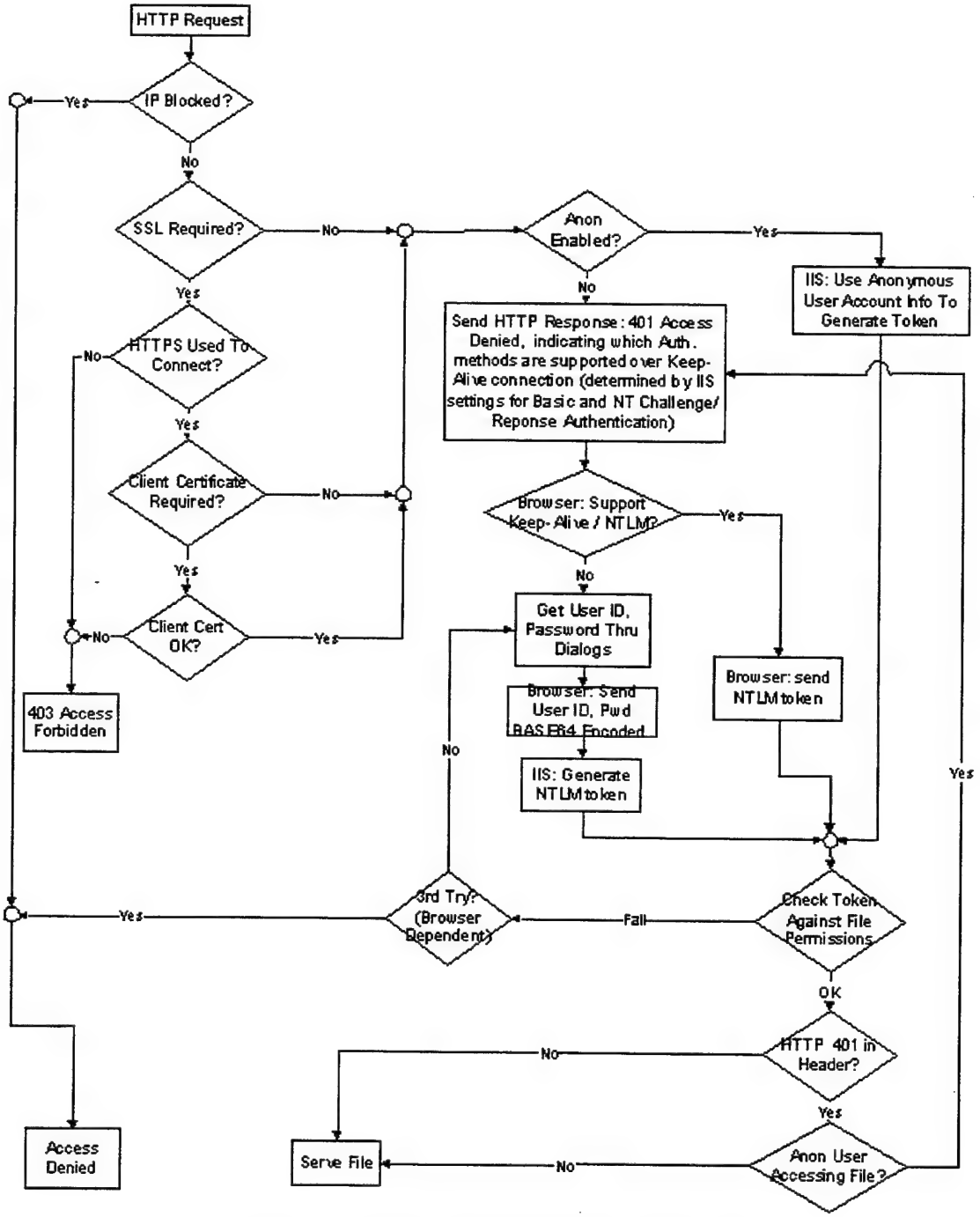

Figure 4.2 File Access Flowchart [Ref. 16]

C. MICROSOFT FRONTPAGE 98

Microsoft® FrontPage 98 is a member of the Microsoft Office family of products, allowing it to integrate easily with NT Server and IIS 4.0. It is touted as the web creation and management tool that requires no programming knowledge but is robust enough for experienced Web site developers. FrontPage can be used to create, edit, and administer web sites to be published by a WWW server. A FrontPage web is a collection of HTML pages, images, documents, and other files and folders that make up a Web site. The main components that will be examined in this chapter include the FrontPage Explorer for managing the web site(s), the FrontPage Editor for creating and editing individual web pages, and the FrontPage Server Extensions.

1. FrontPage Explorer

The FrontPage Explorer is the primary component of the FrontPage application. The Explorer provides the graphical interface to create the layout of a web site. This includes the capabilities to apply a preset graphical theme to the site, organize files and folders, import and export files, test and repair hyperlinks, administer access privileges, track tasks, and launch the FrontPage Editor to design and edit the contents of individual web pages.

a. Administration

FrontPage offers three types of permissions to restrict web pages: browsing, authoring, and administering permissions. Browsing permission allows a user, group of users, or specific workstations to view the specific web from the World Wide

Web. Authoring permission allows a user, group of users, or specific workstations to open the web in FrontPage Explorer and edit pages and files. Administering permission allows a user, group of users, or specific workstations to set permissions for the current web, other users, and computer workstations. All permissions assigned in FrontPage are hierarchical. This means that users with administrative privileges also have authoring and browsing capabilities or a user with authoring permission also has browsing permission. Also, all the FrontPage webs on the web server inherit their initial permissions from the root web by default but can be changed as necessary. The privileges are enforced via the FrontPage Server Extensions discussed later in this chapter.

When permissions are set for a web, the Web server requests a name and password for any task requiring permissions. Some Web servers will authenticate names and passwords by prompting the user or by other means.

b. Views

The Views bar is located at the left of the screen in FrontPage Explorer. Seven buttons provide different ways of looking at information contained in a FrontPage web. The Folders view displays the content of the web arranged by folders and files. In this view, folders and files may be created, deleted, moved, or copied. Figure 4.3 provides an example of the Folders View.

The All Files view displays all the files in a FrontPage web in a list providing information such as the file names, sizes, types, and modification dates.

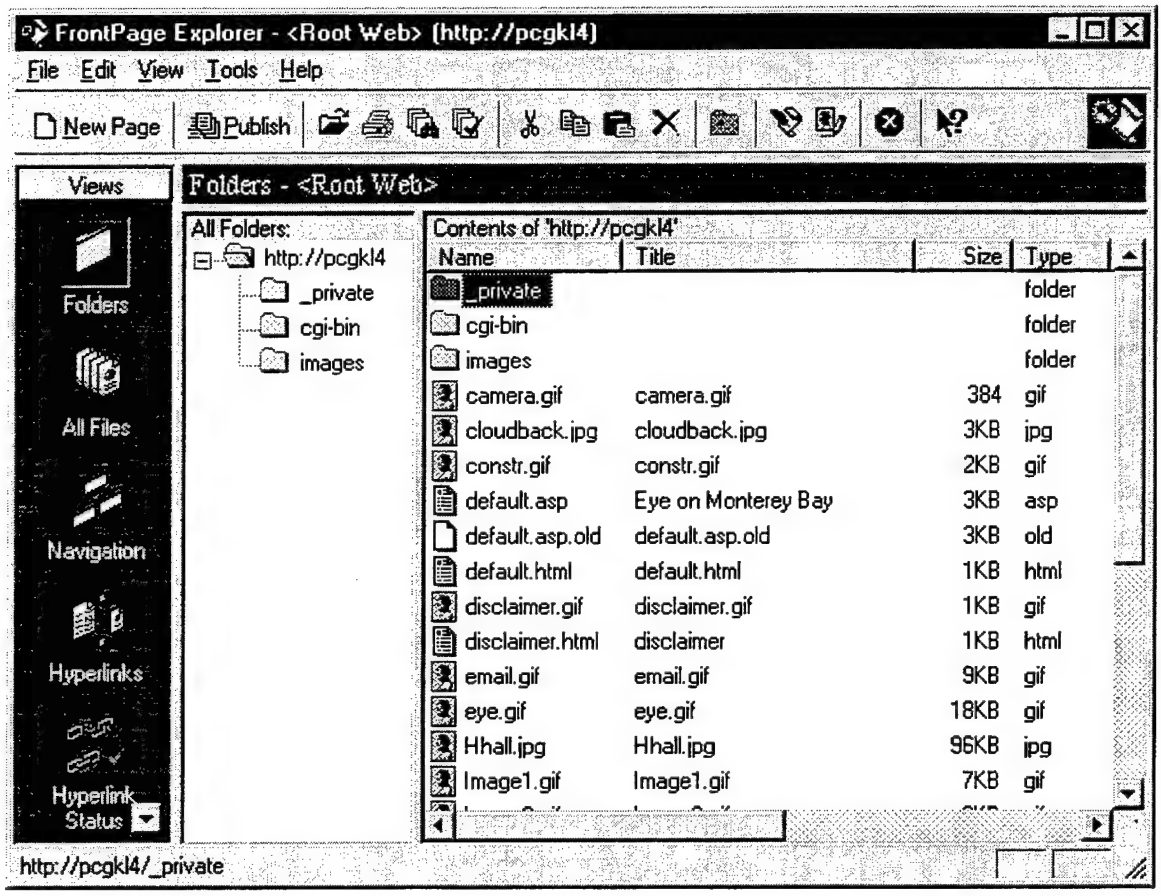

Figure 4.3 FrontPage Explorer Folders View [Ref. 17]

The Navigation view consists of a split-screen display that shows the top-level structure of the FrontPage web in the upper half of the screen and a file and folder list in the lower half of the screen similar to Windows Explorer.

The Hyperlinks view graphically displays hyperlinks to pages and from pages, other files in a FrontPage web, and all hyperlinks from the FrontPage web to other sites on the World Wide Web. The Hyperlink command can be used to create or modify a hyperlink in an existing web. A hyperlink can be created to any page or resource in the current FrontPage web, on a local intranet, or the World Wide Web. If FrontPage

Explorer is used to rename or move a file in the FrontPage web, all hyperlink references to that file are automatically updated within the web, including hyperlinks from Microsoft Office 97 documents. Broken hyperlinks—including hyperlinks to external World Wide Web sites—can also be verified and repaired. Figure 4.4 indicates the structure of the root web hyperlinks.

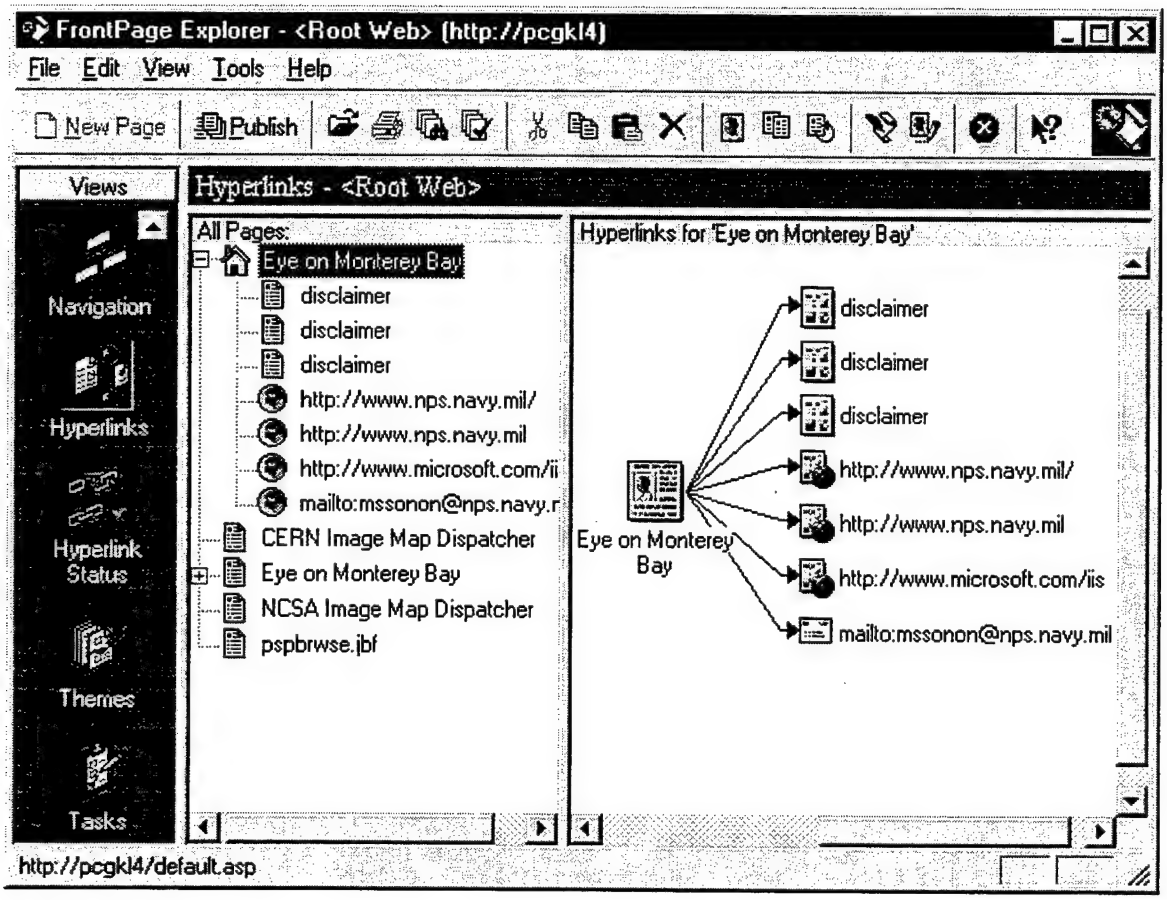

Figure 4.4 FrontPage Explorer Hyperlinks View [Ref. 17]

The Hyperlink Status view identifies the status of the hyperlinks in a FrontPage web. The list includes both internal and external hyperlinks and graphically indicates whether the hyperlinks have been verified or whether they are broken.

The Themes view can be used to apply a set of professionally designed graphics to a FrontPage web. A theme consists of design elements for bullets, fonts, images, navigation bars, and other page elements. When applied, a theme gives the pages and navigation bars in a FrontPage web an attractive and consistent appearance.

The Tasks view in the FrontPage Explorer can track and complete any unfinished FrontPage web tasks, such as spell-checking corrections, on all pages. Clicking a task will automatically redirect the user to the page that needs work. Some tasks are generated automatically during creation and maintenance of a FrontPage web. Other tasks can be added and assigned to other FrontPage authors.

2. FrontPage Editor

While page creation and file management tasks are best handled in the FrontPage Explorer, designing and editing pages is done in the FrontPage Editor. The FrontPage Editor offers an interface similar to a word processor for ease of use. No Hypertext Markup Language (HTML) is required; the FrontPage Editor generates the HTML code from the author's inputs or can convert files from Microsoft Word, Excel, and WordPerfect to HTML. All text, styles, and page formatting are based on Hypertext Markup Language (HTML) standards. Inputs are displayed as they will appear when viewed by a browser. The editor offers many page formats to create HTML pages with the assistance of wizards and templates or allows users to create new templates. The HTML view will also allow an author to edit HTML tags or script code directly.

The editor provides the ability to create and test hyperlinks using a point-and-click interface. Images can be inserted and converted to GIF or JPEG format. Image maps can be created and edited to include hotspots—areas in the image containing hyperlinks. FrontPage image-editing commands allow images to be rotated, cropped, resized, and apply custom enhancements.

3. FrontPage Server Extensions

FrontPage includes a set of programs, called the FrontPage Server Extensions, which are installed on the computer acting as the Web server. The Server Extensions support authoring and administering FrontPage webs. Authoring can include copying or publishing a FrontPage web to other Web servers, creating a table of contents for the web, adding themes and navigational structure to a web, and updating hyperlinks to any pages that have been moved or renamed. Using the Server Extensions, an administrator can assign permissions for a user, group of users, or a specific computer to browse, edit, or administer a FrontPage web. The Server Extensions support browse-time web functionality such as search forms, discussion groups, form processing (including sending form results using e-mail), and other run-time features. [Ref. 18]

The FrontPage client and server extensions are designed to minimize file transfers over the Internet. An author using FrontPage Explorer on a client machine opens a web from the Web server containing the server extensions. Information about the web, such as the hyperlink map, is downloaded to the client machine. The pages and files contained in the web are only downloaded from the Web server when it is opened for editing.

Figure 4.5 shows the FrontPage Server Administrator interface used to administer server extensions on a web.

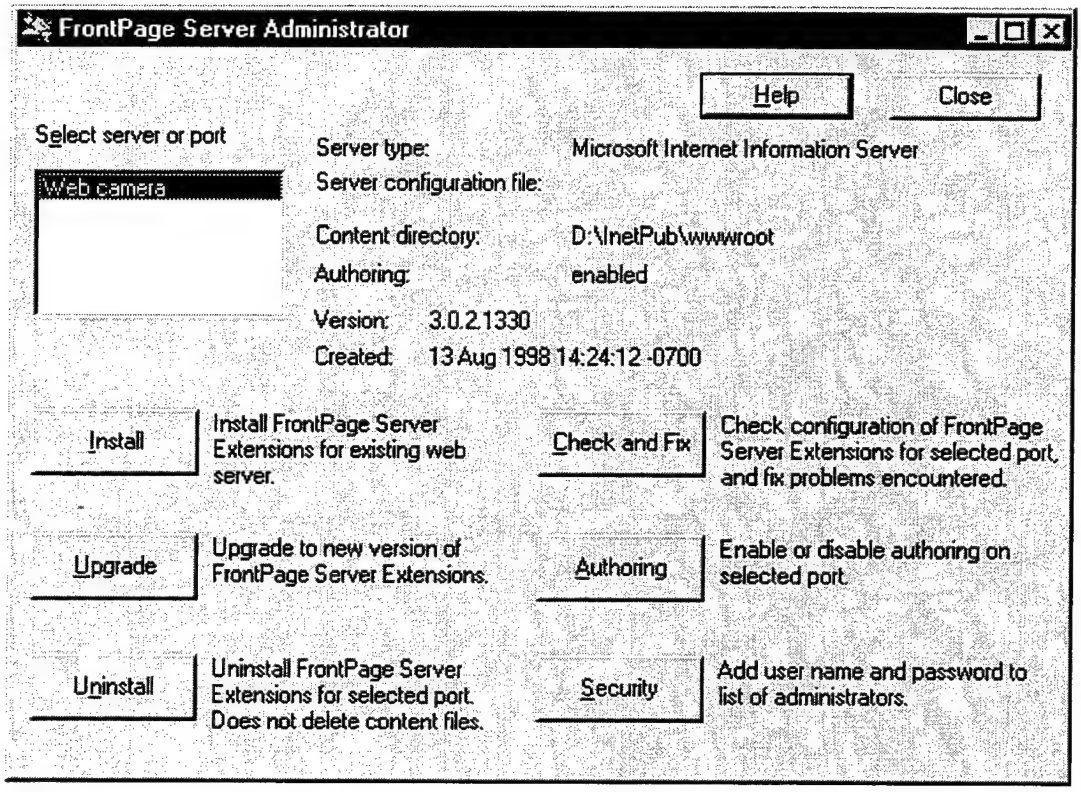

Figure 4.5 FrontPage Server Administrator

The server extensions are designed to work with any standard Web server using the Common Gateway Interface (CGI). Server extensions are developed to be easily portable to popular hardware and software platforms for cross-platform Web server capability. Some FrontPage web features that require server extensions include the full hyperlink map, full-text index of all web pages in the web, a persistent structure defining key pages and resulting relationships between those pages in the FrontPage web, web themes, Tasks list and web-unique security settings. The root web and all sub-webs will

have separate copies of the server extensions installed to enforce end-user, author, and administrator privileges on each web.

The FrontPage client system tools communicate with the server extensions using HTTP. Figure 4.5 displays the interaction between the client system and the server. The client utilizes the Web Extender Client (WEC) library communicating via Winsock and TCP/IP.

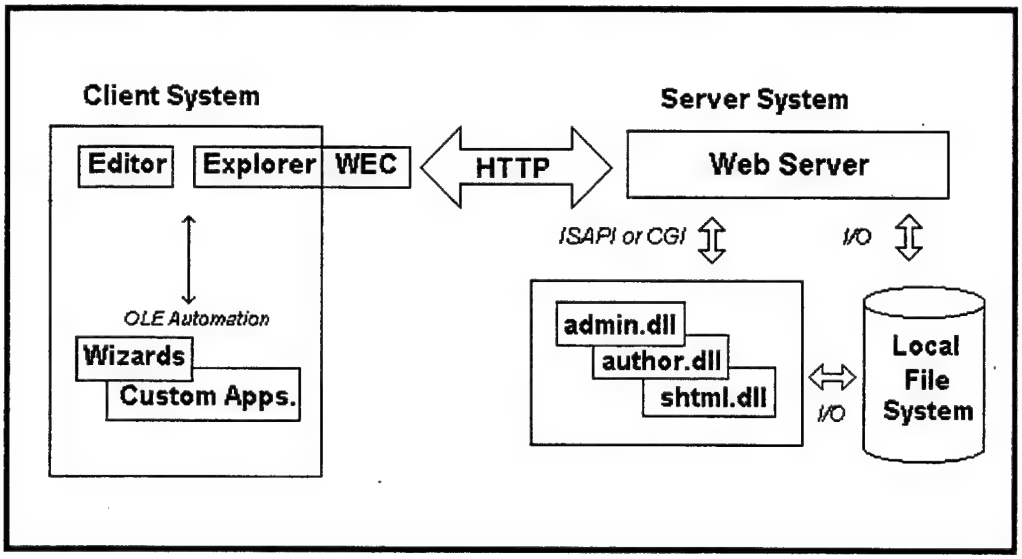

Figure 4.6 FrontPage Server and Client Extensions [Ref. 18]

Each FrontPage web contains copies of the server extensions consisting of three ISAPI DLLs. The DLLs are created in directories below the top-level directory of each web:

- _vti_bin/_vti_adm/admin.dll for administrative tasks,
- _vti_bin/_vti_aut/author.dll for authoring FrontPage webs
- _vti_bin/shtml.dll for browse-time components such as form handlers

All authoring and administrative tasks are performed by sending HTTP POST requests to these DLLs.

Web security is performed on IIS by changing the ACLs for all files and directories in each FrontPage web. The ACL on admin.dll controls who may administer the web. Authoring and browsing permissions are set on author.dll and shtml.dll ACLs, respectively. ACLs for a web are set using the FrontPage Explorer's Permissions command on the Tools menu. As a security measure in Windows NT, a DLL that is called from another DLL must run under the same user account as the calling DLL. Therefore, all system DLL code running due to an IIS request must run in accordance with the user permissions. Since the FrontPage DLLs contain calls to Windows NT system DLLs, FrontPage adds the Interactive and Network accounts to the ACLs of system DLLs called to ensure the correct level of permissions to run under an administrator, author, or user account. The new accounts are provided "read" and "execute" permissions on the system DLLs.

D. CHAPTER SUMMARY

Both Internet Information Server 4.0 and FrontPage 98 are essential to presenting this project on the Internet. The integration with Windows NT 4.0 enables the ability to control access to select components of the web site. This chapter has detailed the role of each of these products from the behind-the-scenes nature of IIS to the content management offered by FrontPage.

V. CERTIFICATES

A. CHAPTER OVERVIEW

This chapter examines the creation, distribution, and use of digital certificates for identification and authentication of servers and clients. In order to control access to specific web pages, this project identifies users using digital certificates.

First, a description of digital certificates in general is presented. Then, two alternatives are presented for implementing access control by issuing certificates to web site users with either Microsoft® Certificate Server or VeriSign™ OnSite.

B. DIGITAL CERTIFICATES DEFINED

Controlling access to resources, whether files or Internet web pages, requires some form of identifying the potential user. Conventional means of identifying users usually involves assigning user accounts with associated passwords.

Passwords may be compromised by transmission over an insecure network, disclosure by the individual, or may be easy to crack by brute force guessing. A strong password policy will correct some deficiencies, but cannot prevent the password from being collected during transmission in the clear over an insecure connection to the server or being disclosed on a note posted near an employee workstation.

A digital certificate can not only provide a fast and efficient means of user identification, but also can save a user from remembering many cumbersome passwords to access different applications on the same server. Certificates are based on public key

cryptography, where a public key is used to encrypt messages that can only be decrypted using the corresponding private key. Because private keys cannot be derived from their corresponding public keys, public keys can be made widely available with no risk to security.

The certificate is basically a document, signed by a trusted certificate authority (CA), which matches public keys to other information such as a name. The CA is a trusted third party that acts almost like a notary public to verify the match between the public keys and the identity of the user, e-mail address, or other information. In order to communicate securely using certificates, the entities must trust the same CA. Certificates signed by that CA are exchanged so the parties involved learn each other's public keys to encrypt and exchange data and verify signatures.

To verify a certificate, the public key of the CA is required and possibly a check against the revocation list. Certificates have a limited life due to changes in the algorithms and protocols and potential compromise of private keys. A certificate is requested, created, and expires or is revoked if compromised. The strength of certificate security depends on the choice and implementation of policy chosen by the CA, the digital algorithms used, the revocation policy used, and the availability and use of certificate revocation lists (CRLs).

1. Security Principles

Certificates enable subscribers to benefit from the following security principles:

a. Identification

Identification offers assurance that senders of digitally signed messages and Web sites are, in fact, who they say they are.

b. Authenticity

Authentication verifies that another party has not altered the message; also called data integrity.

c. Nonrepudiation

Nonrepudiation is the ability for the sender of a signed message to claim that he or she did not send the message, or that he or she sent a different message.

d. Verification

Verification applies to both identification and authentication of a signed message.

e. Privacy

Privacy provides assurance that no one but the recipient can view an encrypted message.

2. Certificate Creation

According to "The Core Technology: Public-Key Cryptography" [Ref. 19], there are six steps to certificate creation.

a. Key Generation

The applicant for a certificate generates a public and a private key.

b. Matching of Policy Information

The applicant packages the additional information necessary for the CA to issue the certificate. The precise definition of the information requested is at the discretion of the CA, but typically includes proof of identity, e-mail address, etc.

c. Sending the Public Keys and Information

The applicant sends the public keys and requested information to the CA, typically encrypted with the CA's public key.

d. Verification of Information

The CA applies its policy governing the verification of the applicant information to determine whether or not to issue a certificate.

e. Certificate Creation

The CA creates a digital document with the appropriate information—public keys, expiration date, etc.—and signs it with the CA's private key.

f. Sending/Posting of Certificate

The CA may send the certificate to the applicant, or post it publicly, as appropriate.

3. X.509 Standard

X.509, or The Directory: Authentication Framework, is an International Telecommunication Union (ITU) recommendation for authentication of directory users in an Open Systems Interconnection (OSI) system. X.509 has formed the basis for most certification schemes used on the Internet. X.509 describes two levels of authentication. These levels are simple authentication—based on usage of a password to verify user identity—and strong authentication, using credentials formed using cryptographic techniques. The standard recommends that only strong authentication be used as the basis of providing secure services.

User certificates may be held within a Directory and may be freely communicated within the system and obtained by users in the same way as other information. X.509 defines a standard structure for certificates that allows for the specification of version and serial numbers, digital signatures, issuer and validity details, subject name and unique identifiers for the issuer and the subject. A method for generating lists of revoked certificates is also defined. The standard allows for one, two and three way authentication. An example of one-way authentication is a client providing identification to a server. Two-way authentication may involve both user and server authentication. Three-way authentication involves a trusted third party to authenticate both the client and the server.

Public-key cryptography is used for strong authentication, but the authentication framework is not dependent on the use of a particular cryptographic algorithm. However,

two users wishing to authenticate must support the same algorithm. The RSA cryptosystem is defined in Annex C of the X.509 standard. Draft amendment 1 to the standard provides additional attributes that can be used to define key identifiers, key policy information, alternative subject or issuer names and certification path constraints.

4. PKCS

Public Key Cryptography Standards (PKCS) govern the are use of public and private digital keys to protect data. PKCS has been developed by RSA Laboratories in cooperation with an informal consortium, originally including Apple, Microsoft, DEC, Lotus, Sun and MIT. The standards have been widely adopted for the specification of security systems based on public and private keys.

PKCS includes both cryptographic algorithm-specific and algorithm-independent implementation standards. Algorithms supported include RSA and Diffie-Hellman key exchange, among others. However, only RSA and Diffie-Hellman are specifically detailed.

PKCS also defines an algorithm-independent syntax for digital signatures, digital envelopes for encryption and extended certificates that enable someone implementing any cryptographic algorithm whatsoever to conform to a standard syntax, and thus achieve interoperability.

To date the following specifications have been published:

- PKCS #1, which defines mechanisms for encrypting and signing data using the RSA public-key cryptosystem.
- PKCS #3, which defines a Diffie-Hellman key agreement protocol.

- PKCS #5, which describes a method for encrypting a string with a secret key derived from a password.
- PKCS #6, which describes a format for extended certificates. An extended certificate consists of an X.509 certificate together with a set of attributes signed by the issuer of the certificate. (PKCS #6 is being phased out in favor of Version 3 of X.509.)
- PKCS #7, which defines a general syntax for messages that include cryptographic enhancements such as digital signatures and encryption.
- PKCS #8, which describes a format for private-key information. This information includes a private key for some public-key algorithm, and optionally a set of attributes.
- PKCS #9, which defines selected attribute types for use in the other PKCS standards.
- PKCS #10, which describes syntax for certification requests.
- PKCS #11, which defines a technology-independent programming interface, called Cryptoki, for cryptographic devices such as smart cards and PCMCIA cards.
- PKCS #12, which defines a Personal Information Exchange Syntax Standard
- PKCS #13, which defines an Elliptic Curve Cryptography Standard.

The specifications used during the course of this project include PKCS #7 and #10.

C. MICROSOFT CERTIFICATE SERVER

Microsoft® Certificate Server 1.0 is a development platform for building Certificate Authorities for enterprises or secure Internet applications. Certificate Server provides customizable services for issuing and managing certificates used in software security systems employing public-key cryptography. A configured and operational CA will allow a site to issue, track, manage, and revoke certificates with minimal

administration overhead. Programmable interfaces are included for developers to create support for additional transports, policies, and certificate properties and formats.

Microsoft Certificate Server must be installed with Microsoft Internet Information Server 4.0 on a server with Windows® NT Server 4.0 with Service Pack 3 installed. Microsoft Internet Explorer version 3.0 or above is required for Web-based certificate enrollment. When installing the certificate server software, a root certificate for the server as a Certificate Authority (CA) will be created. If the "Non-Root CA" option is selected, a certificate request file will be created in order to obtain a certificate from another CA, such as VeriSign™. The Certificate Authority service is configured to start automatically under the System Account when the operating system loads.

Microsoft Certificate Server uses a network share known as the Shared Folder to store the Certificate Server configuration file, CA signature and key exchange certificates, and CA Certificate List Web page. The Shared Folder must be a publicly accessible network share so that any user can access and install the CA certificates using the Certificate Authority Certificate List Web page.

1. Certificate Server Architecture

The Certificate Server consists of a Server Engine, the Server Database, and a set of modules and tools that work together to function as a CA. An operational certification system is composed of four major subsystems: client, intermediary, server, and administrative client. The Figure 5.1 illustrates the relationship between subsystems.

a. Client

The client is the software that is used by the end user to generate a certificate request, send the request, and receive the finished certificate. The client will usually interact with a custom interface maintained by the intermediary application. An example of a client is Microsoft® Internet Explorer version 4.0.

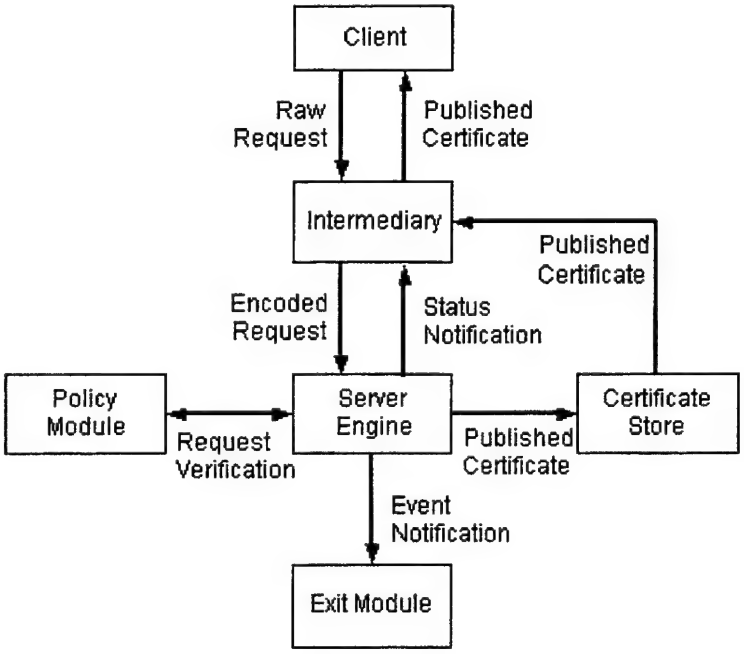

Figure 5.1 Relationships Between Certificate Server Subsystems [Ref. 20]

b. Intermediary

An intermediary subsystem contains the intermediary application and the Certificate Server Client Interface. This application interacts directly with the client, receiving certificate requests and returning finished certificates. It communicates with

the Server Engine through the Certificate Server Client Interface. An example of an intermediary application is Microsoft Internet Information Server.

c. Server

The server is the system that builds the certificate. In addition to the Server Engine, two configurable components are included: the policy module and the exit module.

d. Administrative Client

The administrative client is the system that monitors and manages certificates and requests.

2. Handling Certificate Requests

Certificate Server processes a certificate request in the following manner.

a. Request Reception

The certificate request is received by an intermediary application, which formats it into a PKCS #10 format request and submits it to the Server Engine.

b. Request Approval

The Server Engine calls the Policy Module, which queries request properties, decides whether the request is authorized or not, and sets optional certificate properties.

c. Certificate Formation

If the request is approved, the Server Engine takes the request, and any properties requested by the Policy Module, and builds a complete certificate. The certificate will include the certificate version and serial numbers, digital signature, issuer and validity details, subject name and unique identifiers for the issuer and the subject.

d. Certificate Publication

The completed certificate is then published to a directory service, or given back to the user. By default, the server notifies each exit module installed on the server whenever a certificate is published.

3. Administration

In order to process certificate requests, administer the Certificate Server, and create reports, administrators can access the Certificate Server Web page--depicted in Figure 5.2—containing links to the Certificate Administration Log Utility, the Certificate Administration Queue Utility, Certificate Enrollment Tools, and Certificate Server Documentation. All administrative functions are web-based for ease of use and consistency. However, many functions can also be activated from the command prompt.

The Certificate Enrollment Tools page allows administrators to process certificates requests. The Tools page also permits users to request certificates from the "Request a Client Authentication Certificate" option, obtain, and install a CA certificate in their Web browser from the link to the Certificate Authority (CA) Certificate List Web

page. The Enrollment Tools page will need to be publicly accessible in order to allow new users to submit requests. The Enrollment Tools page is shown in Figure 5.3. The URL to access the Tools page for this system is [http://pcgkl4.ece.nps.navy.mil/CertSrv/CertEnroll/default.htm].

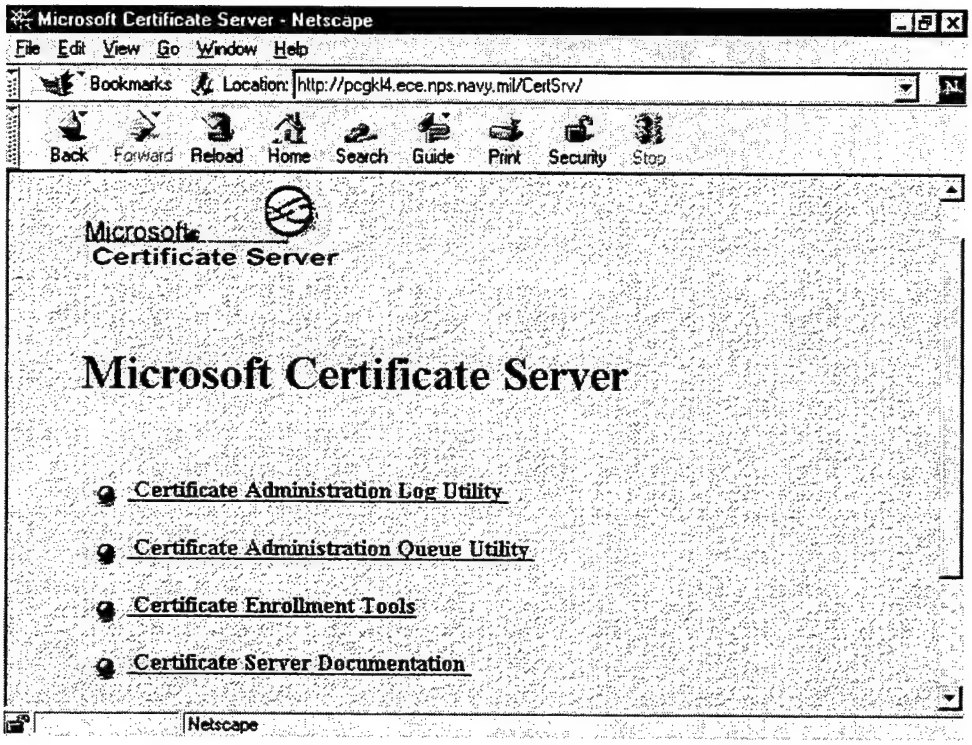

Figure 5.2 Certificate Server Web Page [Ref. 21]

Figure 5.3 Certificate Enrollment Tools Page [Ref. 21]

D. VERISIGN ONSITE

Due to the additional software, database and memory requirements to implement a local certificate server, Microsoft Certificate Server may not be a feasible solution for every system. A trusted third party may be considered to issue and store certificates. In this case, VeriSign, Inc. was chosen as a third party due to a solid reputation as a certificate authority. In addition, VeriSign offers an evaluation copy of the OnSite service in order to test its compatibility with the system used for this project.

VeriSign, Inc. provides a service called OnSite to enable an entity to create, sign and distribute digital certificates without needing to purchase expensive hardware or obtain certificate server software. Individuals, organizations, and devices receiving

certificates are called subscribers. OnSite enables the entity to approve applications for digital certificates for use by individuals or organizations or to issue certificates that identify devices or Web sites. OnSite uses VeriSign's hardware, software, and secure processes and facilities to issue and manage certificates for subscribers. Designated OnSite Certificate Administrators—usually administrators for the web server—approve or reject certificate applications, while a VeriSign CA actually issues the certificates to subscribers from VeriSign's secure facility. Using issued certificates, subscribers can engage in secure electronic communications with the entity server over the Internet.

OnSite End User Certificates support the Secure/MIME (S/MIME) secure email standard. Multipurpose Internet Mail Extensions (MIME) is the official proposed standard for Internet electronic mail. S/MIME is a protocol that adds the digital signature and encryption capabilities of the PKCS to MIME. OnSite Secure Server Certificates are issued as part of a PCKS #7 chain, and may be used to implement Secure Sockets Layer (SSL).

This project utilized an evaluation edition of OnSite in order to test its application to control access to the web site.

1. Onsite Full Setup

A complete version of OnSite supported by VeriSign includes:

- Smartcard and smartcard reader to store the administrative certificate (not included for evaluation copy)
- Configuration wizards to start the service and guide administrators

- Customizable Digital ID extensions that allow inclusion of company name or other information
- Web-based end-user enrollment
- Directory files automatically formatted to support standard-based directories

2. Certificate Application Process

Each applicant takes the following steps to request a certificate from OnSite for access to this web site.

a. Step 1

An applicant for a certificate submits a Web based certificate enrollment form, which includes personal information along with their public key from the URL: [https://testdrive.verisign.com/NavalPostgraduateSchoolCode37/userEnrollNS.htm]. The contents of this enrollment form are encrypted using a medium-grade encryption key (RC4-Export, 128 bit with 40 secret) and securely transferred to OnSite along with the user's public key. OnSite logs the request for Certificate Administrator consideration.

b. Step 2

The OnSite Certificate Administrator uses the smart card to gain secure access to the OnSite Control Center Web site. In the Control Center, the administrator reviews the contents of the certificate application. Using a well-defined process, the administrator can validate the identity and affiliation of the applicant entity.

c. Step 3

If the administrator is able to confirm the information in the enrollment form, the administrator can approve the certificate application. When the administrator indicates approval, OnSite submits a request to the appropriate VeriSign Certification Authority to issue a certificate to the applicant. This request to the CA is digitally signed using the administrator's private key.

d. Step 4

VeriSign's CA creates and signs the certificate. By default, OnSite sends the applicant email notification of certificate approval. The email includes a personal identification number (PIN) and the URL at which the applicant can claim his or her certificate. The default email message is sent to the address provided on the enrollment form and is not encrypted. Administrators can use OnSite's Authentication Wizard to change the method by which the PIN is provided to the end user. The default email message may be used, the message may be sent to a third party to inform the applicant, or a no message option may be selected. If an approval message is not sent, the administrator may notify the applicant personally to receive a PIN by other means.

e. Step 5

Using the PIN, the applicant picks up the certificate. When the applicant accepts the certificate, he or she becomes a subscriber. VeriSign publishes the certificate in its Repository.

3. Certificate Administration

The OnSite Control Center Web pages can be accessed to monitor and manage the lifecycle of issued certificates. Only the OnSite Certificate Administrators are allowed access to the certificates stored at the OnSite Control Center through the public-private key pair and the VeriSign-provided Certificate Administrator certificate that are secured on the included smart card. OnSite enables issuing and administering Private Label End User Certificates, Public Label Secure Server Certificates, and Public Label End User Certificates. A view of the Control Center is provided in Figure 5.4.

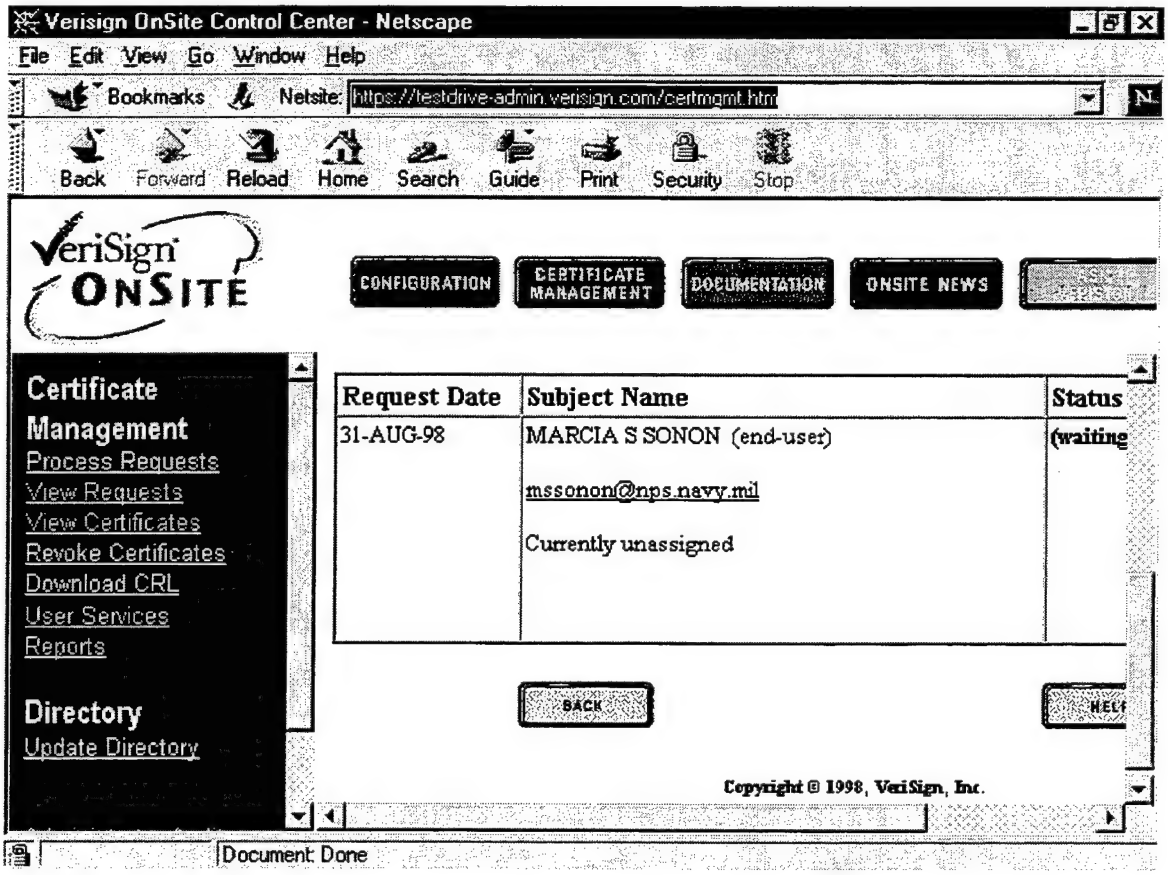

Figure 5.4 VeriSign OnSite Control Center [Ref. 22]

Administrators are given the option to process requests, view requests, view certificates, revoke certificates, download the certificate revocation list (CRL), configure user services such as enrollment and self-revocation of certificates, generate reports, and import certificate directory data files to the local server.

4. Subscribers

After the Certification Authority has issued a certificate, the applicant picks it up using a Web browser or email and installs it in his or her computer. Secure Server Certificates that are issued are installed on the Web server. The user now has a private key in a separate file to which only that subscriber has access, and a public certificate that includes his or her public key and the signature of the issuing CA. The subscriber's public key is made available in the certificate to anyone who wants to correspond with him or her. In the certificate, the public key is bound to a subscriber's name or to a site's fully qualified domain name and to other identifying information requested by the CA.

Privacy of the private key is critical to the proper use of certificates. Therefore, it is essential to convey to subscribers their responsibility for protecting his, her, or its private key(s) from compromise, loss, disclosure, modification, or unauthorized use. Protection may include passwords to protect the certificates kept by the browser a restricted access to stored files, such as keys, in system file storage.

E. CHAPTER SUMMARY

With the increasing use of electronic communication, it is only appropriate that users are no longer required to provide a password that can be easily compromised and

instead are identified by a digital signature. The X.509 standard is widely utilized for digital certificates and is supported by almost all web browsers. In order to control access to files, directories, and web sites, the certificates eliminate the need for multiple passwords and allow a user's certificate to be mapped to a local account on the Windows NT server. Two options are presented for a site to issue certificates. Microsoft Certificate Server allows the issuance and administration of certificates from the system to be accessed. VeriSign offers the OnSite service to customers who wish to issue and administer certificates without the acquisition of additional software and hardware required to maintain and store issued certificates.

VI. HARDWARE SPECIFICATIONS

A. CHAPTER OVERVIEW

This chapter details the specifications of the hardware used for this project.

B. SERVER SETUP

The workstation selected as the project server would be required to be IT-21 compliant in order to achieve the goal of this project. The server would not only need to be the Windows NT domain controller, but also perform the duties of the Web server and certificate server. The server selected for this project is a Dell Dimension XPS R400 personal computer. Table 6.1 lists the hardware specifications of the server.

Component	Specification
Processor	400 MHz Pentium II MMX CPU
Memory	320 MB SDRAM
Data torage/disk drives	8.0 GB Hard Disk Drive 3.5 inch Floppy Disk Drive 24X IDE CD-ROM Iomega Zip 100 drive
Video/Sound	Diamond 8 MB RAM AGP Video Card Soundblaster (Compatible) Audio Card with speakers
NIC	3COM Fast Etherlink XL PCI
SCSI Adapter	Adaptec AHA-2940Ultra Wide
Additional	17 inch Monitor (1280 x 1024) Microsoft Mouse Dell QuietKey Keyboard

Table 6.1 Server Specifications

C. CAMERA

The original goal of the project involved incorporating HTML commands into the web pages that would control a remote system. The "system" selected involves the use of a camera to provide an interactive visual response to commands.

This system uses a Sony DKC-ID1 Pro digital still camera. The camera is connected to the computer by a SCSI cable with a 50 pin connection. The camera package includes a TWAIN software module to interface with the computer and communicate with TWAIN32 compatible software to transfer pictures from the camera to the computer. In order for communication between the camera and computer, the ASPI32 manager (wnaspi32.dll) and the SCSI host adapter device driver (sparrow.mpd/aha154x.mpd/aic78xx.mpd) must be installed in the System folder of the Windows directory.

VII. CONCLUSIONS AND FUTURE WORK

A. THESIS SUMMARY

This thesis explores the concept of implementing IT-2 standards to limit access to a World Wide Web site. The introduction of IT-21 has focused acquisition to primarily Microsoft products to improve interoperability, hence the operating system and applications used for this project.

Microsoft Windows NT Server 4.0 provides the foundation for this task. Chapter III provides and in-depth look at the operating system and the adjustments needed to attain as close to C2 configuration requirements as possible. As long as the system is connected to a network, complete C2 compliance will not be possible. The security measures inherent to NT Server 4.0 are essential to the success of this project.

The software used—Microsoft Internet Information Server 4.0 and FrontPage 98—were chosen for the features each provides, in addition to the ability to integrate with NT Server security measures. Many products offer Internet publishing, but the focus for any DOD system needs to be access control. The solution presented offers a means for allowing any user to browse portions of the site, while restricting access to certain pages. Access control is accomplished through the use of certificates issued by the Microsoft Certificate server or by outside means such as VeriSign's OnSite services. Certificates can be used by the server to identify users, and Windows NT offers the ability to map

certificates to a user account on the server to assign access permissions down to the file level.

B. RECOMMENDATIONS FOR FUTURE WORK

This project can proceed in many areas of future research. Areas originally considered include controlling the functions of the camera itself. This could include focus, zoom, and even controlling movements of the camera. The system is not limited to just a camera as a remote system. The camera interface was chosen for the remote system as a means of visually monitoring changes. The system can be modified for controlling access to specific functions on a web page, not just limiting access to whole pages.

Ideally, this system could be developed to control access to classified and unclassified information on the same site. At this time, the focus has been on limiting access to strictly unclassified information due to the incomplete C2 rating of Windows NT Server 4.0.

APPENDIX A. REGISTRY PERMISSION CHANGES

This appendix contains the following files explaining the contents of the recommended C2regacl.inf and C2ntfacl.inf files to be used with Microsoft's C2 Configuration Manager. The registry changes are made when the "Registry Security" option is activated. The file and permission changes are implemented by activating the "File System Security" option.

In the case that C2 Configuration Manager is not operable, the registry and file permission changes may be instituted manually.

C2REGACL.INF

```
; * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
;    Modified C2regacl.inf file by
;    NSA Windows NT Integration Team
;    01 DEC 97
;
;   Registry ACL definition file
;
;   Use this file to set the registry key ACL's to the
;   desired security. The format of each entry is:
;
;       [RegistryKey]
;       Domain\Account = [INHERIT,] access [, access]...
;
;   where:
;
;     RegistryKey is the key path of the key to set. This
;     is in the format of:
;
;           PREDEFINED_KEY\[path | *]
;       where:
;
;           PREDEFINED_KEY is one of:
;               HKEY_LOCAL_MACHINE
;               HKEY_USERS
;               HKEY_CURRENT_USER
;               HKEY_CLASSES_ROOT
;
;         and path is the path to the key. The path may end
;         in a "*" character in which case, all sub-keys of
;         the specified path will be set to the specified
;         security
;
;       for example:
;
;           [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\*]
;
;               would assign the security description of
;               that section to all keys UNDER the
;               HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
;               key but NOT to the
;               HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
;               key itself. To assign security to that key,
;               an entry such as the following would be
;               needed:
```

```
;
;                [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft]
;
;
;    Domain\Account
;        specifies the account to recieve the specified
;        access for that key. Account may be an account or a
;        group. For Example to give permissions to all
;        administrator accounts, the:
;
;            BUILTIN\Administrators
;
;        would be the correct entry.
;
;    access is defined as one of the following:
;
;        QV   = Query Value
;        SV   = Set Value
;        CS   = Create Subkey
;        ES   = Enumerate Subkeys
;        NT   = Notify
;        CL   = Create Link
;
;        DE   = Delete
;        RC   = Read Control
;        WD   = Write DAC
;        WO   = Write Owner
;
;    there are also some predefined combination access keys:
;
;        NONE = no access
;        FULL = QV, SV, CS, ES, NT, CL, DE, WD, WO, RC
;        READ = QV, ES, NT, RC
;
;    The 'INHERIT' string can be specified (in the first
;    entry only) to indicate this is the access control to
;    be assigned by default to created subkeys.
;
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *

[HKEY_LOCAL_MACHINE\SOFTWARE]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes]
BUILTIN\Administrators = FULL
```

```
SYSTEM = FULL
Authenticated Users = Read

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\*]
BUILTIN\Administrators = FULL
BUILTIN\Administrators = INHERIT, FULL
SYSTEM = FULL
SYSTEM = INHERIT, FULL
Authenticated Users = Read
Authenticated Users = INHERIT, Read

[HKEY_LOCAL_MACHINE\SOFTWARE\Description]
BUILTIN\Administrators = FULL
BUILTIN\Administrators = INHERIT, FULL
SYSTEM = FULL
SYSTEM = INHERIT, FULL
CREATOR OWNER =  FULL
CREATOR OWNER =  INHERIT, FULL
Authenticated Users = QV, SV, CS, ES, NT, DE, RC
Authenticated Users = INHERIT, QV, SV, CS, ES, NT, DE, RC

[HKEY_LOCAL_MACHINE\SOFTWARE\Description\*]
BUILTIN\Administrators = FULL
BUILTIN\Administrators = INHERIT, FULL
SYSTEM = FULL
SYSTEM = INHERIT, FULL
CREATOR OWNER =  FULL
CREATOR OWNER =  INHERIT, FULL
Authenticated Users = QV, SV, CS, ES, NT, DE, RC
Authenticated Users = INHERIT, QV, SV, CS, ES, NT, DE, RC

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft]
BUILTIN\Administrators = FULL
SYSTEM = FULL
CREATOR OWNER =  FULL
Authenticated Users = QV, SV, CS, ES, NT, DE, RC

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\*]
BUILTIN\Administrators = FULL
BUILTIN\Administrators = INHERIT, FULL
SYSTEM = FULL
SYSTEM = INHERIT, FULL
CREATOR OWNER =  FULL
CREATOR OWNER =  INHERIT, FULL
Authenticated Users = QV, SV, CS, ES, NT, DE, RC
Authenticated Users = INHERIT, QV, SV, CS, ES, NT, DE, RC
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Program Groups]
BUILTIN\Administrators = FULL
CREATOR OWNER =  FULL
SYSTEM = FULL
BUILTIN\Power Users = QV, SV, CS, ES, NT, DE, RC
Authenticated Users = READ

[HKEY_LOCAL_MACHINE\SOFTWARE\Secure]
BUILTIN\Administrators = FULL
CREATOR OWNER =  FULL
SYSTEM = FULL
Authenticated Users = READ

[HKEY_LOCAL_MACHINE\SOFTWARE\Windows 3.1 Migration Status]
BUILTIN\Administrators = FULL
BUILTIN\Administrators = INHERIT, FULL
CREATOR OWNER =  FULL
CREATOR OWNER =  INHERIT, FULL
SYSTEM = FULL
SYSTEM = INHERIT, FULL
Authenticated Users = READ
Authenticated Users = INHERIT, READ

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\RPC]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AeDebug]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Compatibility]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Drivers]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Embedding]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Font Cache]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Font Drivers]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Font Mapper]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Fonts]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\FontSubstitutes]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\GRE_Initialize]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\MCI]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\MCI Extensions]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\PerfLib]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Port]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Profile List]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Type1 Installer]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read


[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\WOW]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Shares]
BUILTIN\Administrators = FULL
```

```
SYSTEM = FULL
Authenticated Users = Read

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\UPS]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureP
ipeServers]
BUILTIN\Administrators = FULL
SYSTEM = FULL

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersio
n\Run]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersio
n\RunOnce]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersio
n\Uninstall]
BUILTIN\Administrators = FULL
SYSTEM = FULL
Authenticated Users = Read
```

C2NTFACL.INF

```
; * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
;    Modified C2ntfacl.inf file by
;    NSA Windows NT Integration Team
;    01 DEC 97
;
;   File System ACL definition file
;
;   Use this file to set the ACL's on files and directories
;   to the desired
;   security. The format of each entry is:
```

```
;
;       [DirPath]
;       Domain\Account = [Predefined Access |
;                         FileAccessString [, DirAccessString]]
;
;       [FilePath]
;       Domain\Account = [Predefined Access |
;                         FileAccessString]
;
;   where:
;
;     FilePath is the path of the file or directory to set.
;     This is in the format of a file path name. The file
;     path may contain environment variables (such as
;     %systemroot%) which will be expanded on the system
;     running tha application.
;
;     The last item in the FilePath string may be a
;     directory, file, wildcard file or an exclamation
;     ("!"). In the case of an exclamation all files and
;     sub-directories of the preceeding path will be set to
;     the specified security.
;
;       for example:
;
;           [%systemroot%\system32\!]
;
;               would assign the security description of
;               that section to all files and sub-
;               directories UNDER the %systemroot\system32
;               directory as well as to the
;               %systemroot\system32 directory itself. To
;               assign security to just the files in that
;               directory , an entry such as the following
;               would be needed:
;
;               [%systemroot%\system32\*.*]
;
;
;   Domain\Account
;       specifies the account to recieve the specified
;       access for that file. Account may be an account or
;       a group. For Example to give permissions to all
;       administrator accounts, the:
;
;           BUILTIN\Administrators
;
```

```
;       would be the correct entry.
;
;   access string is defined as one of the following:
;
;       a combination of access chars
;
;       access
;       char  File Access        Dir Access
;       ----  ----------------   ----------------
;       R     = Read Data        List Directory
;       W     = Write Data       Add File
;       X     = Execute File     Traverse Directory
;       D     = Delete           Delete
;       P     = Change Perms     Change Perms
;       O     = Take Ownership   Take Ownership
;
;       e.g. SYSTEM = RWXD
;
;
;   there are also some predefined combination access keys:
;
;       NONE = no access
;       ALL = RWXDPO
;
;   Standard Directory & File access references are:
;
;       Access           Access Granted
;       Name             (Dir)(File)
;       -----------      ------------------
;       FullControl =    (ALL)(ALL)
;       Change      =    (RWXD)(RWXD)
;       AddRead     =    (RWX)(RX)
;       Read        =    (RX)(RX)
;       Add         =    (WX)(none specified)
;       List        =    (RX)(none specified)
;       NoAccess    =    (NONE)(NONE)
;
;
;   * * * * * * * * * N O T E * * * * * * * * * * * * * * *
;
;   For correct application of the access control, the more
;   restrictive access entries must be placed ahead of (on
;   top of) the more permissive access. The correct "sort"
;   order would be:
;
;       NoAccess, List, Add, Read, AddRead, Change,
;       FullControl
```

```
;
;
; * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
;
;   NOTE: the security items are applied from the top of
;   the file to the bottom. Because of that, top level
;   directory entries with more restrictive security should
;   be at the top of the file and less restrictive entries
;   to specific users and/or specific files should be
;   listed next.
;
; * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *


[%SystemDrive%\]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
CREATOR OWNER = FullControl
SYSTEM = FullControl


[%SystemDrive%\*.*]
Authenticated Users = change
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemDrive%\IO.SYS]
Authenticated Users = read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemDrive%\MSDOS.SYS]
Authenticated Users = read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemDrive%\BOOT.INI]
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemDrive%\NTDETECT.COM]
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemDrive%\NTLDR]
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
```

```
[%SystemDrive%\AUTOEXEC.BAT]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemDrive%\CONFIG.SYS]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemDrive%\TEMP\!]
Authenticated Users = add
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl

[%SystemDrive%\USERS\!]
Authenticated Users = List
BUILTIN\Administrators = RWXD
SYSTEM = FullControl

[%SystemDrive%\USERS\DEFAULT]
Authenticated Users = RWX
CREATOR OWNER = FullControl
SYSTEM = FullControl

[%SystemDrive%\WIN32APP\!]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl
SERVER OPERATOR = FullControl

[%SystemRoot%\!]
Authenticated Users = List
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl


[%SystemRoot%\Config\!]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl
```

```
[%SystemRoot%\Cursors\!]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl

[%SystemRoot%\Fonts\!]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl

[%SystemRoot%\Help\!]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl

[%SystemRoot%\inf\!]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl

[%SystemRoot%\Media\!]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl

[%SystemRoot%\Pif\!]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl

[%SystemRoot%\ShellNew\!]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl

[%SystemRoot%\system\!]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl
```

```
SERVER OPERATOR = FullControl

[%SystemRoot%\system32\!]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl

[%SystemRoot%\Profiles]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl

[%SystemRoot%\*.*]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl

[%SystemRoot%\*.INI]
Authenticated Users = change
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemRoot%\WIN.INI]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemRoot%\WINFILE.INI]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemRoot%\SYSTEM.INI]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemRoot%\ODBCINST.INI]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemRoot%\ODBC.INI]
Authenticated Users = Read
```

```
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemRoot%\LOCALMON.DLL]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
BUILTIN\Power Users = change

[%SystemRoot%\PRINTMAN.HLP]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
BUILTIN\Power Users = change

[%SystemRoot%\REPAIR\!]
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemRoot%\SYSTEM\*.*]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl
SERVER OPERATOR = FullControl

[%SystemRoot%\SYSTEM32]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl

[%SystemRoot%\SYSTEM32\*.*]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl
SERVER OPERATOR = FullControl

[%SystemRoot%\SYSTEM32\rdisk.exe]
BUILTIN\Administrators = FullControl
SERVER OPERATORS = read
SYSTEM = FullControl

[%SystemRoot%\system32\regedt32.*]
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
```

```
[%SystemRoot%\SYSTEM32\rcp.*]
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemRoot%\SYSTEM32\rsh.*]
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemRoot%\SYSTEM32\AUTOEXEC.NT]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemRoot%\SYSTEM32\CMOS.RAM]
Authenticated Users = read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemRoot%\SYSTEM32\CONFIG.NT]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemRoot%\SYSTEM32\MIDIMAP.CFG]
Authenticated Users = read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemRoot%\SYSTEM32\PASSPORT.MID]
Authenticated User = FullControl
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemRoot%\SYSTEM32\CONFIG\!]
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemRoot%\SYSTEM32\DHCP\!]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
BUILTIN\Power Users = change
CREATOR OWNER = FullControl

[%SystemRoot%\SYSTEM32\DRIVERS\!]
Authenticated Users = Read
```

```
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl
SERVER OPERATORS = FullControl

[%SystemRoot%\SYSTEM32\OS2\!]
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemRoot%\SYSTEM32\RAS]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
BUILTIN\Power Users = change
CREATOR OWNER = FullControl

[%SystemRoot%\SYSTEM32\RAS\*.*]
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemRoot%\SYSTEM32\REPL\!]
Authenticated Users = List
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl
SERVER OPERATORS = FullControl

[%SystemRoot%\SYSTEM32\REPL\EXPORT\!]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl
SERVER OPERATORS = change
BUILTIN\Replicator = change

[%SystemRoot%\SYSTEM32\REPL\IMPORT\!]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl
SERVER OPERATORS = change
BUILTIN\Replicator = change

[%SystemRoot%\SYSTEM32\SPOOL\!]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
```

```
CREATOR OWNER = FullControl
BUILTIN\Power Users = change
SERVER OPERATORS = FullControl
PRINT OPERATORS = FullControl

[%SystemRoot%\SYSTEM32\WINS\!]
Authenticated Users = list
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemDrive%\NTRESKIT\!]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl

[%SystemDrive%\Program Files\!]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl

[%SystemRoot%]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl

[%SystemRoot%\ShellNew\*.*]
Authenticated Users = Read
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl

[%SystemRoot%\Profiles\Administrator\!]
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
CREATOR OWNER = FullControl

[%SystemRoot%\regedit.*]
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemRoot%\$NtServicePackUninstall$\!]
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
```

```
[%SystemRoot%\$NtUninstall*\!]
BUILTIN\Administrators = FullControl
SYSTEM = FullControl

[%SystemRoot%\SendTo\!]
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
Authenticated Users = Read


[%SystemDrive%\ffastun*.*]
BUILTIN\Administrators = FullControl
SYSTEM = FullControl
```

APPENDIX B. USER RIGHTS RECOMMENDATIONS

The table on the following pages defines the user rights for Windows NT Server and includes a compilation of the recommendations for configuration from the *Guide to Implementing Windows NT® in Secure Network Environments* by the National Security Agency [Ref. 5] and "Securing Microsoft Windows NT Installation" by the Microsoft® Corporation [Ref. 7]. User rights are allowable actions which can be assigned to users or groups in addition to the built-in abilities. Careful allocation of standard and advanced user rights can significantly strengthen the security of an NT system.

Standard/Advanced User Rights Recommendations

	Policy [Regular (R), Advanced (A)]	NTS Default	Navy Configuration for NT Servers
1.	**Access this computer from the network (R):** Allows a user to connect over the network to the computer	Administrators Authenticated Users	Administrators Authenticated Users
2.	**Act as part of the operating system (A):** Allows a process to perform as a secure, trusted part of the operating system. Some subsystems are granted this right.	(None)	(None)
3.	**Add workstations to domain (R):** Allows users to added workstations to a particular domain. This right is meaningful only on domain controllers.	(None)	(None)
4.	**Back up files and directories (R):** Allows a user to back up files and directories. This right supersedes file and directory permissions.	Administrators Backup Operators Server Operators	Administrators Backup Operators Server Operators
5.	**Bypass traverse checking (A):** Allows a user to change directories and access files and subdirectories even if the user has no permission to access parent directories.	Everyone	(None)
6.	**Change the system time (R):** Allows a user to set the time for the internal clock of the computer.	Administrators Server Operators	Administrators Server Operators
7.	**Create a pagefile (A):** Allows the user to create new pagefiles for virtual memory swapping.	Administrators	Administrators
8.	**Create a token object (A):** Allows a process to create access tokens. Only the Local Security Authority can do this.	(None)	(None)

	Policy [Regular (R), Advanced (A)]	NTS Default	Navy Configuration for NT Servers
9.	**Create permanent shared objects (A):** Allows user to create special permanent objects, such as \\Device, that are used within Windows NT.	(None)	(None)
10.	**Debug programs (A):** Allows a user to debug various low-level objects such as threads.	Administrators	(None)
11.	**Force shut down from a remote system (R):** Allows the user to shutdown a Windows NT system remotely over a network.	Administrators Server Operators	Administrators Server Operators
12.	**Generate security audits (A):** Allows a process to generate security audit log entries.		(None)
13.	**Increase quotas (A):** Nothing. This right has no effect in current versions of Windows NT.	Administrators	Administrators
14.	**Increase scheduling priority (A):** Allows a user to boost the execution priority of a process.	Administrators	Administrators
15.	**Load and unload device drivers (R):** Allows a user to install and remove device drivers.	Administrators	Administrators
16.	**Lock pages in memory (A):** Allows a user to lock pages in memory so they cannot be paged out to a backing store such as Pagefile.sys.	(None)	(None)
17.	**Log on as a batch job (A):** Nothing. This right has no effect in current versions of Windows NT.	(None)	(None)

	Policy [Regular (R), Advanced (A)]	NTS Default	Navy Configuration for NT Servers
18.	**Log on as a service (A):** Allows a process to register with the system as a service.	(None)	(None)
19.	**Log on locally (R):** Allows a user to log on at the computer, from the computer's keyboard.	Account Operators Administrators Backup Operators Print Operators Server Operators	Account Operators Administrators Backup Operators Print Operators Server Operators
20.	**Manage auditing and security log (R):** Allows a user to specify what types of resource access (such as file access) are to be audited, and to view and clear the security log. Note that this right does not allow a user to set system auditing policy using the Audit command in the Policy menu of User Manager. Also, members of the administrators group always have the ability to view and clear the security log.	Administrators	Administrators
21.	**Modify firmware environment values (A):** Allows a user to modify system environment variables stored in nonvolatile RAM on systems that support this type of configuration.	Administrators	Administrators
22.	**Profile single process (A):** Allows a user to perform profiling (performance sampling) on a process.	Administrators	Administrators
23.	**Profile system performance (A):** Allows a user to perform profiling (performance sampling) on the system.	Administrators	Administrators

	Policy [Regular (R), Advanced (A)]	NTS Default	Navy Configuration for NT Servers
24.	**Replace a process level token (A):** Allows a user to modify a process's security access token. This is a powerful right used only by the system.	(None)	(None)
25.	**Restore files and directories (R):** Allows a user to restore backed-up files and directories. This right supersedes file and directory permissions.	Administrators Backup Operators Server Operators	Administrators Backup Operators Server Operators
26.	**Shut down the system (R):** Allows a user to shut down Windows NT.	Account Operators Administrators Backup Operators Print Operators Server Operators	Account Operators Administrators Backup Operators Print Operators Server Operators
27.	**Take ownership of files or other objects (R):** Allows a user to take ownership of files, directories, printers, and other objects on the computer. This right supersedes permissions protecting objects.	Administrators	Administrators

LIST OF REFERENCES

1. Clemins, Admiral Archie. "IT-21:The Path to Information Superiority," *Chips*, July, 1997. http://www.chips.navy.mil/chips/archives/97_jul/file1.htm

2. Message 300944Z MAR 97 from CINCPACFLT. Subject: INFORMATION TECHNOLOGY FOR THE 21ST CENTURY.

3. "The Foundations of Microsoft Windows NT System Architecture," Microsoft Corporation, September, 1997.

4. Goncalves, Marcus. *Windows NT 4.0 Server Security Guide*, Upper Saddle River, NJ: Prentice Hall, Inc., 1998.

5. National Security Agency, *Guide to Implementing Windows NT® in Secure Network Environments*, December 1997.

6. National Computer Security Center, *Microsoft Windows NT Version 3.5 Final Evaluation Report*, June 23, 1995.

7. "Securing Microsoft Windows NT Installation," Microsoft Corporation, August, 1997.

8. Hutt, Arthur E., Seymour Bosworth, and Douglas B. Hoyt. *Computer Security Handbook*, New York: John Wiley & Sons, Inc., 1995.

9. Russell, Deborah and G.T. Gangemi, Sr. *Computer Security Basics*, Sebastopol, CA: O'Reilly & Associates, Inc., 1991.

10. Microsoft Windows NT C2 Configuration Manager, Microsoft Windows NT Server Resource Kit 4.0, Microsoft Press.

11. Department of the Navy, Space and Naval Warfare Systems Command, Naval Information Systems Security Office, *Secure Windows NT Installation and Configuration Guide*, Version 1.2., June, 1998. http://infosec.navy.mil/COMPUSEC/NTSECURE.HTML

12. Microsoft® User Manager for Domains, Version 4.0, Microsoft Corporation, 1996.

13. Microsoft Knowledge Base Article Q161990. http://support.microsoft.com/support/kb/articles/q161/9/90.asp

14. Bergmann, Ken. "A High-Level Look at Microsoft Internet Information Server," Microsoft Deveolpment Network Technology Group, Microsoft Corporation, November, 1995.

15. "Supporting Microsoft® Internet Information Server," Microsoft Press, 1996.

16. Enfield, Paul. "Implementing a Secure Site with ASP," Microsoft Corporation, October, 1997.

17. Microsoft® FrontPage Explorer, Version 3.0.2.1330, Microsoft Corporation, 1997.

18. "An Overview of the FrontPage Server Extensions," Microsoft® MSDN™ Library, Microsoft Corporation, July 1998.

19. "The Core Technology: Public-Key Cryptography," Microsoft Corporation, September, 1996.

20. "Processing Certificate Requests," Microsoft® MSDN™ Library, Microsoft Corporation, July 1998.

21. Microsoft® Certificate Server, Version 1.0, Microsoft Corporation, 1997.

22. "VeriSign™ OnSiteSM 3.0 Certificate Administrator's Handbook," Version 2.12, VeriSign, Inc., 1998. http://www.verisign.com/onsite/doc/adminBook/admin.html

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Rd., Ste 0944
   Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, CA 93943-5101

3. Dan C. Boger, Dean 2
   Computer and Information Science and Operations
   Naval Postgraduate School
   Monterey, CA 93942-5000

4. Gus K. Lott, Assistant Professor 2
   Electrical and Computer Engineering Department Code EC/lt
   Naval Postgraduate School
   Monterey, CA 93942-5000

5. Daniel F. Warren, Assistant Professor 2
   Computer Science Department Code CS/Wd
   Naval Postgraduate School
   Monterey, CA 93942-5000

6. LT Marcia Sonon, USN 2
   953 Pine Street
   Hamburg, PA 19526